Richmond Journal of Law and Technology

Volume 16 | Issue 1 Article 3

2009

"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Necessity of Measures to Avoid Identity Fraud After a Data Breach

James Graves

"MEDICAL" MONITORING FOR NON-MEDICAL HARMS: EVALUATING THE REASONABLE NECESSITY OF MEASURES TO AVOID IDENTITY FRAUD AFTER A DATA BREACH

By: James Graves*

Cite as: James Graves, *"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Necessity of Measures to Avoid Identity Fraud After a Data Breach*, XVI RICH. J.L. & TECH. 2 (2009), http://law.richmond.edu/jolt/v16i1/article2.pdf

I. INTRODUCTION

[1] In July 2005, "reformed" hacker Albert Gonzalez noticed an insecure wireless network at a Marshalls department store in Miami.[1] After exploiting the vulnerability, Gonzalez and his accomplices installed programs that captured credit card numbers.[2] They stored the credit card numbers on servers in Latvia and Ukraine, created ATM cards using some of the numbers, and used those cards to withdraw hundreds of thousands

* J.D. Candidate 2010, William Mitchell College of Law; M.S., Information Networking, Carnegie Mellon University, 2004; B.S., Mathematics/Computer Science, Carnegie Mellon University, 1994. The author gratefully acknowledges advice from Professor David J. Prince.

[1] Brad Stone, *Global Trail of an Online Crime Ring*, N.Y. TIMES, Aug. 12, 2008, at A1, *available at* http://www.nytimes.com/2008/08/12/technology/12theft.html (reporting federal indictments against Mr. Gonzalez). After an arrest on credit-card fraud charges in 2003, Gonzalez made a deal to avoid prison time by helping federal agents track down credit-card traffickers. *See id*.

[2] *Id.*

of dollars in cash.[3] Fifteen months later, Marshalls' parent company, TJX, announced that forty-five million of its customers' credit card numbers had been exposed to the thieves.[4]

[2] Data broker ChoicePoint collects information on nearly every adult in the United States.[5] It gathers and aggregates data anywhere it can find it, including motor vehicle records, police records, property records, court records, and credit histories.[6] These records include all the details necessary to set up new credit accounts, such as Social Security numbers, birth dates, addresses, mothers' maiden names, and driver's license numbers.[7] In 2004, ChoicePoint discovered that some clients who had claimed to be small businesses were actually data thieves.[8] A year later, ChoicePoint admitted to selling hundreds of thousands of records to these thieves.[9] As a result, over 800 people suffered identity fraud.[10]

---

[3] *Id.*

[4] *Id*. Gonzalez was arrested in his hotel room in May, 2008. *Id.* At the time of his arrest, his hotel room contained two laptops, over $20,000 in cash, and a gun. *Id.*

[5] Gary Rivlin, *Keeping Your Enemies Close: The Rehabilitation Of a Data Company*, N.Y. TIMES, Nov. 12, 2006, at B1, *available at* http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html. ChoicePoint was spun off from credit reporting agency Equifax in 1997. *Id.*

[6] *See id.*

[7] *Id.*

[8] *See* Tom Zeller, Jr., *Release of Consumers' Data Spurs ChoicePoint Inquiries*, N.Y. TIMES, Mar. 5, 2005, at C2, *available at* http://www.nytimes.com/2005/03/05/business/05choice.html.

[9] Rivlin, *supra* note 5.

[10] *See id.*; Press Release, Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Sept. 28, 2009).

[3] These examples illustrate how data collection can lead to identity fraud.[11] The chain of events begins when an organization collects sensitive data. At some point, a breach occurs, and the organization loses control of that data. When a third party obtains and misuses the breached information, harms result. Identity fraud, often called "identity theft",[12] is one of the main forms of these harms.[13]

[11] *See, e.g.*, N. MITCHISON ET AL, EUROPEAN COMM'N JOINT RESEARCH CTR. IDENTITY THEFT: A DISCUSSION PAPER 5 (2004), https://prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[12] The term "identity theft" is popularly used to describe frauds resulting from misuse of identifying data. *See, e.g.*, Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH L.J. 237, 241–44 (2004). However, others have used the term "identity fraud," and the entire field of research suffers from a lack of agreement on exactly what "identity theft" is. *See, e.g.*, MITCHISON, *supra* note 11, at 5; FIDIS CONSORTIUM ON D5.2B: ID-RELATED CRIME: TOWARDS A COMMON GROUND FOR INTERDISCIPLINARY RESEARCH 5, 10–15 (2006), http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf; Bob Sullivan, *Just How Common is ID Theft?*, MSNBC, June 30, 2005, http://www.msnbc.msn.com/id/8409283 (last visited Sept. 28, 2009) (noting that surveys of identity theft disagree on the definition of the term). This note uses the term "identity fraud," except when referring to decisions in court cases where the more common term is used. "Identity theft" is not theft and it does not involve one's identity. *See* L. JEAN CAMP, ECONOMICS OF IDENTITY THEFT: AVOIDANCE, CAUSES AND POSSIBLE CURES 17 (2007). As some commentators have pointed out, an identity is more like intellectual property than real property in that most "identity theft" cases involve copying identifying information, not stealing it. *See, e.g.*, FIDIS CONSORTIUM, *supra*, at 5, 10–15. The word "identity" is also debatable. Most cases of fraud exploit poor methods of *authenticating* identity, not the victim's actual identity. *See id*. Many discussions of the topic also confuse *identity* with *identification*. One's identity is more than just a set of data about that person. *See, e.g.*, Stacey L. Schreft, *Risks of Identity Theft: Can the Market Protect the Payment System?*, FED. RESERVE BANK OF KAN. CITY ECON. REV., Oct. 2007, at 5, 6, *available at* http://www.kansascityfed.org/Publicat/Econrev/PDF/4q07schreft.pdf. To paraphrase Yoda: luminous beings are we, not this crude data. *See* GEORGE LUCAS, LAURENCE KASDAN & LEIGH BRACKETT, STAR WARS EPISODE V: THE EMPIRE STRIKES BACK (1980), *available at* http://www.imsdb.com/scripts/Star-Wars-The-Empire-Strikes-Back.html (last visited Sept. 28, 2009).

[13] *See* discussion *infra* Part V.A.

[4] Consumers who find out that their data has been mishandled respond in a number of ways. Some simply ignore the breach notice.[14] Some avail themselves of a free year or two of credit monitoring, a customary offering by breached organizations.[15] Some want more than a year or two of credit monitoring—and some of those sue the breached organization for those costs.[16]

[5] One theory put forward in these lawsuits is that negligent organizations should pay for the costs of monitoring to detect or prevent identity fraud.[17] Plaintiffs have analogized these "data monitoring" claims to the medical monitoring claims in toxic torts.[18] Among other similarities, both claims involve initial exposures that can lead to remote harms.[19] So far, however, courts have rejected this analogy.[20]

[6] This article examines the arguments for and against recovery of data monitoring costs. Part II gives some background on the claims, first highlighting attempts to recover monitoring costs after data breaches, then discussing medical monitoring claims and some of the benefits and problems with these claims. Part III compares data monitoring claims to medical monitoring claims by examining the analogy and comparing the

---

[14] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 952 (2007) (noting that more than thirty-nine percent of respondents in a survey said they had mistaken a breach notification letter for junk mail).

[15] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 35 (2007) [hereinafter 2007 GAO Report] (noting that it has become "standard practice" for entities that experience a breach to offer free credit monitoring after a breach).

[16] *See* discussion, *infra* Part II.A.

[17] *See id.*

[18] *See id.*

[19] *See id.*

[20] *See id.*

underlying policy arguments for each. Part IV proposes a model for evaluating non-medical monitoring claims based on whether those costs were reasonably necessary. Part V then applies this model to data monitoring costs by examining the costs and probabilities involved, and shows that these do not currently justify awarding the costs of data monitoring.

II. BACKGROUND

A. DATA BREACH SUBJECTS' ATTEMPTS TO RECOVER THE COSTS OF RESPONDING TO A BREACH

[7] Because identity fraud may not develop until years after a data breach,[21] data breach victims have used a number of novel theories in attempting to recover damages for the breaches themselves. Plaintiffs have sought recovery for increased risk of identity fraud,[22] fear of identity fraud,[23] and cost of efforts to reduce their risk of identity fraud.[24] These

[21] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1234–38 (2003); *Identity Theft: Restoring Your Good Name: Hearings Before the S. Subcomm. on Technology, Terrorism, and Government Information*, 107th Cong. 12 (2003) (statement of Howard Beales, Director, FTC Bureau of Consumer Protection) (testifying that five percent of identity theft victims were unaware of the theft five years after it happened, and that the average time to detect an identity theft was twelve months).

[22] *See, e.g.*, Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1125 (N.D. Cal. 2008); Shafran v. Harley-Davidson, Inc., No. 07 Civ. 01365(GBD), 2008 WL 763177, at *1 (S.D.N.Y. Mar. 20, 2008); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 4 (D.C. 2007); Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793, 796 (M.D. La. 2007); Key v. DSW, Inc., 454 F. Supp. 2d 684, 686 (S.D. Ohio 2006).

[23] *See, e.g.*, Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873, 874 (E.D. La. 2008); Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629, 632 (7th Cir. 2007); *Ponder*, 522 F. Supp. 2d at 796.

[24] *See, e.g.,* Pinero v. Jackson-Hewitt Tax Serv., Inc., 594 F. Supp. 2d 710, 714 (E.D. La. 2009); *Shafran*, 2008 WL 763177, at *1; *Pisciotta*, 499 F.3d at 632; Stollenwerk v. Tri-West Health Care Alliance, 254 Fed.Appx. 664, 665 (9th Cir. 2007); *Randolph*, 486 F. Supp. 2d at 4; Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 709 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006);

claims mimic, respectively, the toxic tort theories of enhanced risk, fear of future harm, and medical monitoring.[25] Although these theories have gained some acceptance in the context of physical harms,[26] they have proven much less helpful for data breach plaintiffs. Few of these claims have survived summary judgment or motions to dismiss.[27]

[8] Courts have rejected these claims for a number of reasons. Many found the harm too speculative to confer standing, especially when plaintiffs claimed increased risk or emotional harms.[28] Even when plaintiffs have sought the cost of measures to avoid identity fraud, courts typically have found these efforts not to be harms themselves, but merely voluntary actions taken in anticipation of potential future harm.[29] Some

Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3 (D. Minn. Feb. 7, 2006); Giordano v. Wachovia Sec., LLC, No. 06-476 (JBS), 2006 WL 2177036, at *2 (D.N.J. July 31, 2006); *Key*, 454 F. Supp. 2d at 686.

[25] *See generally* L. NEAL ELLIS, JR. & CHARLES D. CASE, TOXIC TORT AND HAZARDOUS SUBSTANCE LITIGATION §§ 6-1 to 6-4 (1995).

[26] *See* discussion *infra* Part II.B.

[27] *See, e.g.*, *Pinero*, 594 F. Supp. 2d at 718–19 (granting summary judgment to defendant for contract claims including expenses for credit monitoring); *Kahle,* 486 F. Supp. 2d at 709–13 (granting summary judgment to defendant where plaintiff argued for the cost of credit monitoring as a harm); *Giordano*, 2006 WL 2177036, at *5 (remanding to state court for lack of standing, where plaintiff's only claimed harm was the cost of money spent to prevent identity fraud); *Key*, 454 F. Supp. 2d at 685 (dismissing a claim seeking recovery for the increased risk of identity fraud). *But see* Lambert v. Hartman, 517 F.3d 433, 438 (6th Cir. 2008) (finding that a plaintiff who alleged identity fraud had standing to sue for the cost of credit monitoring); *Ruiz,* 540 F. Supp. 2d at 1126 (holding that a pre-trial motion to dismiss was too early a stage to dismiss a claim for increased risk of identity fraud because such a risk could be proven as part of the plaintiff's case).

[28] *See, e.g.*, *Ponder*, 522 F. Supp. 2d at 796–98; *Randolph*, 486 F. Supp. 2d at 8–9; *Forbes*, 420 F. Supp. 2d at 1020–21; *Guin*, 2006 WL 288483 at *3–6.

[29] *See Ponder*, 522 F. Supp. 2d at 796–98; *Randolph*, 486 F. Supp. 2d at 8; *Forbes*, 420 F. Supp. 2d at 1020–21.

courts have done little more than survey other states' positions on credit monitoring as a compensable injury.[30]

[9] But a handful of courts have considered, at least briefly, the similarity between claims for medical monitoring and claims for credit monitoring. In *Giordano v. Wachovia Securities, L.L.C.*,[31] the U.S. District Court for the District of New Jersey became the first court to consider the analogy, deeming it "inapt."[32] Just over a month later, in *Key v. DSW, Inc.*,[33] the U.S. District Court for the Southern District of Ohio followed suit. Two other federal courts have noted the analogy when rejecting claims.[34]

[10] The most extensive judicial analysis of the analogy to date appears in a case by the U.S. Court of Appeals for the Ninth Circuit, *Stollenwerk v. Tri-West Health Care Alliance*.[35] The *Stollenwerk* court denied a claim for credit monitoring damages to plaintiffs whose data was on a computer stolen from Tri-West because the plaintiffs had not shown that the breached information was misused in any way.[36] The court held that even

---

[30] *See Pinero*, 594 F. Supp. 2d at 715–17; Shafran v. Harley-Davidson, Inc., No. 07 Civ. 01365(GBD), 2008 WL 763177, at *1–3 (S.D.N.Y. Mar. 20, 2008).

[31] No. 06-476, 2006 WL 2177036 (D. N.J. July 31, 2006).

[32] *Id.* at *3 n.4. The court rejected the analogy because it found that the plaintiff's allegation of potential identity fraud resulting from data loss was merely an allegation of *potential* exposure, not an allegation of *actual* exposure required for a medical monitoring claim. *Id.*

[33] 454 F. Supp. 2d 684, 691 (S.D. Ohio 2006) (finding a lack of exposure because plaintiff did not allege that her data had been misused).

[34] *See* Pisciotta v. Old Nat'l Bank Corp., 499 F.3d 629, 639 (7th Cir. 2007); Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006). The courts in both these cases were applying state law in states that did not recognize claims for medical monitoring, and thus found it unlikely that the states would have recognized claims for non-medical monitoring costs. *See id.*; *Pisciotta*, 499 F.3d at 639.

[35] 254 Fed. Appx. 664 (9th Cir. 2007).

[36] *Id.* at 666–67.

if credit monitoring damages were available under the same standard as medical monitoring claims, the plaintiffs had failed to meet that standard because they did not show that the relief sought was necessary.[37] The court also discussed one of the underlying justifications for medical monitoring damages: "to ensure that the cost of testing does not prevent plaintiffs from receiving increased medical surveillance that is of actual benefit to them."[38] The court rejected the claims because the plaintiffs had not shown that "a normally prudent person in these circumstances" would have purchased credit monitoring services beyond those that Tri-West offered for free.[39]

[11] Other than *Stollenwerk*, courts considering the parallel between identity monitoring claims and medical monitoring damages have focused primarily on the analogy, with particular attention to the issue of exposure.[40] But this analysis skips a step. The question should not be merely whether data breach is or is not like toxic exposure. The inquiry should instead be based on an evaluation of the arguments for and against medical monitoring damages and their applicability in the data breach context.

B. MEDICAL MONITORING

1. OVERVIEW

[12] Medical monitoring damages allow recovery of the costs of medical tests designed to detect and prevent the onset of diseases resulting

[37] *Id*.

[38] *Id.* at 667.

[39] *Id.*

[40] *See, e.g.*, Giordano v. Wachovia Secs., L.L.C., No. 06-476, 2006 WL 2177036, at *3 n.4 (D.N.J. July 31, 2006); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690–91 (S.D. Ohio 2006).

from the a defendant's actions.[41] Plaintiffs have sought damages for the cost of monitoring the long-term effects of physical injuries,[42] pharmaceuticals,[43] tobacco,[44] insecticides,[45] asbestos,[46] and other harmful substances.[47] Although standards for medical monitoring damages vary across jurisdictions, a few common elements have emerged. Recovery of medical monitoring costs requires proof that (1) the plaintiff was exposed to a toxic substance,[48] (2) the exposure resulted from the defendant's negligence,[49] (3) the exposure increased[50] the plaintiff's risk of serious

[41] *See* Richard Bourne, *Medical Monitoring Without Physical Injury: The Least Justice Can Do for Those Industry Has Terrorized with Poisonous Products*, 58 SMU L. REV. 251, 252 (2005).

[42] *See, e.g.*, Friends for All Children, Inc. v. Lockheed Aircraft Corp., 746 F.2d 816, 818–19 (D.C. Cir. 1984).

[43] *See, e.g.*, Petito v. A.H. Robins Co., 750 So. 2d 103, 103 (Fla. Dist. Ct. App. 1999).

[44] *See, e.g.*, Lowe v. Philip Morris USA, Inc., 183 P.3d 181, 182 (Or. 2008).

[45] *See, e.g.*, Villari v. Terminix Int'l, Inc., 663 F. Supp. 727, 728 (E.D. Pa. 1987).

[46] *See, e.g.*, Burns v. Jaquays Mining Corp., 752 P.2d 28, 33 (Ariz. Ct. App. 1987) (allowing damages for procedures to detect and treat diseases arising from asbestos exposure).

[47] *See, e.g.*, *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 835 (3d Cir. 1990) (poly-chlorinated biphenyls); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 800 (Cal. 1993) (carcinogenic toxic waste); Ayers v. Twp. of Jackson, 525 A.2d 287, 292 (N.J. 1987) (various toxic chemicals).

[48] Hansen v. Mountain Fuel Supply Co., 858 P.2d 970, 979 (Utah 1993). Some jurisdictions use a higher standard that requires proof of *significant* exposure. *See, e.g.*, *Paoli*, 916 F.2d at 852; Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 432 (W. Va. 1999).

[49] *See, e.g.*, *Paoli*, 916 F.2d at 852 (listing "negligent actions of the defendant" as a component of the court's medical monitoring test); *Hansen*, 858 P.2d at 979 (including "exposure . . . caused by the defendant's negligence" in the elements of a valid medical monitoring claim); *Bower*, 522 S.E.2d at 432 (allowing medical monitoring for exposure that results from the defendant's "tortious conduct").

disease or illness,[51] (4) there exist beneficial medical procedures to treat that disease or illness,[52] and (5) those procedures are reasonably necessary.[53]

[13] One of the biggest differences in the approaches to medical monitoring claims is whether recovery depends on the plaintiff having a present physical injury. States with a present-physical-injury requirement allow recovery for medical monitoring only when the plaintiff has

[50] *Hansen*, 858 P.2d at 979. Some jurisdictions phrase their tests as requiring a "significant" increase. *See, e.g.*, *Paoli*, 916 F.2d at 852; *Bower*, 522 S.E.2d at 432. This stronger language does not appear to make a substantive difference. *See Bower*, 522 S.E.2d at 432 (holding a "significant" increase in risk does not have to be more probable than not, only higher than the risk without exposure).

[51] Jurisdictions agree that the disease or illness for which the plaintiff is at risk must be serious. *See, e.g.*, *Hansen*, 858 P.2d at 979 (phrasing this element as requiring a serious risk of disease, illness, *or injury*); *Bower*, 522 S.E.2d at 432.

[52] The requirement that the medical procedures be beneficial takes several forms. *Compare Paoli*, 916 F.2d at 852 (requiring the monitoring and testing procedures simply be "beneficial"), *with Hansen*, 858 P.2d at 979 (holding that early detection is beneficial if a treatment can alter the course of an illness), *and Bower*, 522 S.E.2d at 433 (having no explicit requirement that the procedure be beneficial, but instead relying on the reasonable necessity element to serve the same function).

[53] Courts have also stated the reasonable necessity requirement in different ways. Some simply say that the medical procedures must be reasonably necessary. *Compare Paoli*, 916 F.2d at 852 (requiring medical examinations to be only reasonably necessary), *and* Ayers v. Twp. of Jackson, 525 A.2d 287, 312 (N.J. 1987) (holding that medical surveillance must merely be "reasonable and necessary"), *with Hansen*, 858 P.2d at 979 (requiring that monitoring be prescribed by a qualified physician according to contemporary scientific principles), *and Bower*, 522 S.E.2d at 433 (explaining that a medical procedure is reasonably necessary if a qualified physician would prescribe that procedure). Jurisdictions also differ on whether cost should factor into the analysis. *Compare Bower*, 522 S.E.2d at 433 (holding that "factors such as financial cost and the frequency of testing need not necessarily be given significant weight" in determining whether a procedure is reasonably necessary) *with Hansen*, 858 P.2d at 980 (noting that a procedure's costs might outweigh its benefits because "excessive price," among other reasons).

manifested some physical harm.[54] Of the twenty-nine states that recognize medical monitoring claims,[55] sixteen allow recovery only when the plaintiff has shown a present physical injury.[56]

2. BENEFITS

[14] Many of the benefits of allowing medical monitoring claims arise from public health interests. Recognition of medical monitoring claims reflects the widely accepted value of early diagnosis and treatment in preventing disease,[57] and that money alone cannot fully compensate a victim for loss of health.[58] These public health benefits are some of the most commonly cited reasons for allowing medical monitoring claims.[59]

---

[54] In some but not all states, the requirement is for a present physical *injury*—not only must there be a demonstrable physical condition traceable to the exposure, but that condition must be harmful. *See, e.g.*, Parker v. Brush Wellman, Inc., 420 F. Supp. 2d 1355, 1361–62 (N.D. Ga. 2006). Other states, however, allow medical monitoring when there is a physical condition proving exposure, even if that condition is not strictly a disease or injury. *See id.* (listing several jurisdictions that do and do not consider asymptomatic pleural thickening to be an "injury" sufficient to allow recovery of medical monitoring costs).

[55] *See* D. Scott Aberson, Note, *A Fifty-State Survey of Medical Monitoring and the Approach the Minnesota Supreme Court Should Take when Confronted with the Issue*, 32 WM. MITCHELL L. REV. 1095, 1114–17 (2006). As of 2006, twenty-nine states plus the District of Columbia, Guam, and the Virgin Islands allowed medical monitoring claims. *See id*. Since then, Mississippi and Oregon have both considered and rejected claims for medical monitoring without present physical injuries. *See* Paz v. Brush Eng'red Materials, Inc., 949 So. 2d 1, 7 ¶ 20 (Miss. 2007); Lowe v. Philip Morris USA, Inc., 183 P.3d 181, 186–87 (Or. 2008).

[56] Aberson, *supra* note 55, at 1114.

[57] *See Ayers*, 525 A.2d at 311–12.

[58] *See* Heidi Li Feldman, *Harm and Money: Against the Insurance Theory of Tort Compensation*, 75 TEX. L. REV. 1567, 1576 (1997).

[59] *See, e.g.*, Burns v. Jaquays Mining Corp., 752 P.2d 28, 33–34 (Ariz. Ct. App. 1987) (quoting *Ayers*, 525 A.2d at 311); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993); Miranda v. Shell Oil Co., 26 Cal. Rptr. 2d 655, 660 (Ct. App. 1993);

[15] Recovery for medical monitoring costs also improves deterrence.[60] Exposure can take decades to develop into disease[61]—too far in the future for potential liability to be a factor when business decisions are often based on short-term profits.[62] By the time the disease develops, the company responsible for the release of toxins might not even be in business.[63] Not only could payments for medical procedures could happen early enough to figure into business calculations, but the shorter time frame for medical monitoring claims also allows the plaintiff a better chance to prove causation than she would have when the disease is diagnosed years or decades after exposure.[64]

[16] Medical monitoring recovery has been justified on other grounds. One consideration is simple equity: when a victim has been exposed to toxins as a result of a wrongdoer's negligence, the wrongdoer, not the victim, should shoulder the cost of reasonably necessary medical

Hansen v. Mountain Fuel Supply Co., 858 P.2d 970, 976–77 (Utah 1993) (quoting *Ayers*, 525 A.2d at 311).

[60] *Potter*, 863 P.2d at 824.

[61] *See Miranda*, 26 Cal. Rptr. at 659–60 (discussing claims that might be precluded when "disease actually develops, years, perhaps decades" into the future); Greenville v. W.R. Grace & Co., 827 F.2d 975, 978 (4th Cir. 1987) (noting that asbestos-related diseases "may not develop until decades after exposure"); BARRY I. CASTLEMAN, ASBESTOS: MEDICAL AND LEGAL ASPECTS 91 (1984) (discussing a 1960 study that found that "[t]he average time from onset of exposure to development of cancer was 25 years for lung cancer with asbestosis, and 30 years for peritoneal cancer.").

[62] M. P. Narayanan, *Managerial Incentives for Short-Term Results,* 40 J. FIN. 1469, 1469 (1985).

[63] *See* Thomas J. Salerno et al., *Environmental Law and Its Impact on Bankruptcy Law—Saga of "Toxins-R-Us",* 25 REAL PROP. PROB. & TR. J. 261, 263 (1990); Anthony G. Hopp, *Bad Medicine: The Legal, Policy and Medical Arguments Against Medical Monitoring*, 23 BNA TOXICS L. REP. 436, 436–40 (2008).

[64] *Ayers*, 525 A.2d at 311–12. This deterrence function also has a secondary health benefit: deterring release and use of toxins reduces the number of infections and thus overall public health. *See id.* at 312.

procedures.[65] Another consideration is cost: many diseases that result from toxic exposure are expensive to treat; procedures for early detection can save money.[66]

[17] The doctrine of avoidable consequences provides another cost-related justification. [67] Somewhat incorrectly referred to as a "duty to mitigate," [68] the doctrine prevents a plaintiff from recovering damages she could have avoided with reasonable effort.[69] A toxic tort plaintiff would therefore be unable to recover any amount that was avoidable through reasonably necessary detection and prevention procedures.[70] Allowing the plaintiff to recover the costs of those procedures recognizes that she is expected to do so.[71]

---

[65] *See id*. at 311.

[66] *See id.* at 312; Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993). *But see* discussion *infra* note 90.

[67] *See Ayers*, 525 A.2d at 310–11 (noting that under the doctrine of avoidable consequences, failure to submit to medically advisable treatment "may bar future recovery for a condition he could thereby have alleviated or avoided."); *see also* discussion *infra* Part IV.B.

[68] The doctrine of avoidable consequences is a defense allowing reduction of damages; it does not create a duty on the part of the plaintiff to the defendant. *See* Jeffrey K. Riffer & Elizabeth Barrowman, *Recent Misinterpretations of the Avoidable Consequences Rule: The "Duty" To Mitigate and Other Fictions*, 16 HARV. J.L. & PUB. POL'Y 411, 415–17 (1993).

[69] *See* RESTATEMENT (SECOND) OF TORTS § 918(1) (1979); *see also* JACOB A. STEIN, STEIN ON PERSONAL INJURY DAMAGES § 18:1 (3d ed. 2009).

[70] *Ayers*, 525 A.2d at 310–11. Note, however, that courts do not always require plaintiffs to submit to medical procedures to mitigate damages. *See* STEIN, *supra* note 69 § 18:4.

[71] *See* discussion *infra* Part IV.B.

3. PROBLEMS

[18] Despite these benefits, medical monitoring claims have several problems. Some of the problems stem from the uncertainty inherent in a claim based on monitoring for future harm.[72] In most cases, a toxic exposure only increases the risk of a future harm; it neither guarantees harm nor necessarily creates a significant probability of harm.[73] Some courts, therefore, find the costs of monitoring to be too speculative to convey standing or count as a compensable injury.[74] Courts that allow medical monitoring claims—especially those that allow claims without a showing of present physical injury—reason that the relevant injury is the need for monitoring itself, provided that the plaintiff can show that such monitoring is medically prudent.[75]

---

[72] Metro-N. Commuter R.R. Co. v. Buckley, 521 U.S. 424, 442 (1997).

[73] *See, e.g.*, Wood v. Wyeth-Ayerst Labs., 82 S.W.3d 849, 854 (Ky. 2002) (noting that the plaintiff's exposure had the "potential to result in serious future medical consequences" but had not yet done so).

[74] *See, e.g.*, *id.* at 856 (holding that allowing medical monitoring absent a showing of present physical injury would enable litigation based on "speculative fears of future injury"); Hinton v. Monsanto Co., 813 So. 2d 827, 830 (Ala. 2001) (holding that "a cause of action based upon nothing more than an increased risk that an injury or an illness might one day occur would result in the courts of this State deciding cases based upon nothing more than speculation and conjecture").

[75] *See In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 851 (3d Cir. 1990) (holding that " the appropriate inquiry is not whether it is reasonably probable that plaintiffs will suffer harm in the future, but rather whether medical monitoring is, to a reasonable degree of medical certainty, necessary in order to diagnose properly the warning signs of disease."); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993) (emphasizing that "allowing compensation for medical monitoring costs 'does not require courts to speculate about the probability of future injury. It merely requires courts to ascertain the probability that the far less costly remedy of medical supervision is appropriate.'"); Ayers v. Twp. of Jackson, 525 A.2d 287, 311 (N.J. 1987) (holding that medical monitoring damages are available "provided that plaintiffs can establish with a reasonable degree of medical certainty that such expenditures are 'reasonably anticipated' to be incurred by reason of their exposure"); Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 430 (W. Va. 1999).

[19] Similarly, the indeterminate nature of exposure to toxins raises serious concerns about the number of potential plaintiffs in a medical monitoring case.[76] For example, when a polluter releases toxins into the environment or when a widely traveled area contains asbestos, it is difficult to draw lines between who has been "exposed" and who has not.[77] Critics of medical monitoring point out that nearly everyone is exposed to toxins,[78] and argue that allowing recovery of medical monitoring costs for mere exposure would create a flood of lawsuits that could crush the legal system.[79] A flood of relatively minor cases would also prevent the courts from devoting their limited resources to the most worthy claims.[80]

[20] The present-physical-injury requirement addresses some of these concerns. An existing physical injury shows the harm necessary for

[76] *See Buckley*, 521 U.S. at 442.

[77] *See id.* (expressing concern that "tens of millions of individuals may have suffered exposure to substances that might justify some form of substance-exposure-related medical monitoring").

[78] *See id*. at 434–35 (listing statistics showing extensive public exposure to carcinogens); *see also* Susan L. Martin & Jonathan D. Martin, *Tort Actions for Medical Monitoring: Warranted or Wasteful?*, 20 COLUM. J. ENVTL. L. 121, 130 (1995) ("in the very near future we may all have reasonable grounds to allege that some negligent business exposed us to hazardous substances."); Hopp, *supra* note 63, at 439 ("[i]f negligently exposing someone to a hazardous substance gives rise to a legal claim, then every person in the United States would daily have a long list of potential lawsuits to choose from.").

[79] *Buckley*, 521 U.S. at 442. *See also* James A. Henderson, Jr. & Aaron D. Twerski, *Asbestos Litigation Gone Mad: Exposure-Based Recovery for Increased Risk, Mental Distress, and Medical Monitoring*, 53 S.C. L. REV. 815, 845 (2002) ("[a]nother inescapable implication of the inherent vagueness and open-endedness of medical monitoring litigation is that the courts will face, in the long run, an overwhelming flood of litigation in this area.").

[80] *Buckley*, 521 U.S. at 443–44 (expressing concern that a medical monitoring cause of action would degrade "a tort system that can distinguish between reliable and serious claims on the one hand, and unreliable and relatively trivial claims on the other.").

standing and negligence.[81] It also limits the potential class of plaintiffs to those who have manifested physical symptoms, eliminating would-be plaintiffs who can only allege proximity to a toxin, not infection.[82]

[21] Another problem with medical monitoring claims is the potential risk inherent in medical monitoring procedures. Many of these procedures are invasive and carry health risks that must be weighed against the procedures' potential benefits.[83] In addition to the risks from the procedures themselves, there are risks that patients may take false reassurance from the monitoring, or that false positives could lead to unnecessary, costly, or dangerous follow-up procedures.[84] A related question is whether a toxic exposure really makes monitoring procedures more necessary than they would have been otherwise. Some level of monitoring is prudent even without any exposure to a toxin;[85] it would be inequitable to require a defendant to pay for medical procedures the plaintiff should have received regardless of exposure. Juries and judges, therefore, face the difficult task of determining the amount of monitoring needed as a result of the defendant's actions over and above the normally prudent level.[86]

---

[81] *See, e.g.*, Hinton v. Monsanto Co., 813 So. 2d 827, 832 (Ala. 2001); Wood v. Wyeth-Ayerst Labs., 82 S.W.3d 849, 859 (Ky. 2002); Paz v. Brush Eng'red Materials, Inc., 949 So. 2d 1, 9 ¶ 25(Miss. 2007); Aberson, *supra* note 55, at 1114.

[82] *See* Henry v. Dow Chem. Co., 701 N.W.2d 684, 690 (Mich. 2005) (explaining that the physical injury requirement "defines more clearly who actually possesses a cause of action").

[83] *See* Victor E. Schwartz, Leah Lorber & Emily J. Laird, *Medical Monitoring: The Right Way and the Wrong Way*, 70 MO. L. REV. 349, 356–57 (2005) (discussing the risks of monitoring procedures).

[84] *Id.*

[85] *See Buckley*, 521 U.S. at 441–42 (citing expert testimony that the American Cancer Society recommends periodic colon cancer screening for everyone).

[86] *See id.* (noting the difficulty in getting experts to agree on whether extra monitoring is medically necessary as the result of toxic exposure).

[22] Courts have addressed these risk and necessity questions by relying on expert medical opinions.[87] The medical opinions should take risk factors into account.[88] In theory, a doctor would only prescribe testing procedures when the benefits of those procedures outweigh their risks. Expert medical testimony can also help establish how much monitoring is necessary as a direct result of the alleged exposure.[89]

[23] Other criticisms of medical monitoring claims involve cost factors. Because medical tests can be expensive, courts have expressed concern that these procedures could be much more expensive than the illnesses the procedures are meant to detect.[90] Making defendants pay for the costs of medical tests also ignores alternative forms of payment for these procedures, such as insurance.[91] Some courts and commentators worry

[87] In some jurisdictions, this is satisfied if tests are found to be "reasonably necessary," defined as procedures that a qualified physician would prescribe. *See* Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 433 (W. Va. 1999). Others jurisdictions require the actual prescription of the monitoring procedures. *See, e.g.*, Hansen v. Mountain Fuel Supply Co., 858 P.2d 970, 980 (Utah 1993). *Hansen*'s prescription requirement ensures that a medical procedure not only exists and is theoretically beneficial, but that a doctor has determined that the procedure is "medically advisable for that plaintiff." *Id.*

[88] The medical necessity of a procedure may or may not involve its monetary cost, depending on jurisdiction. *See* discussion *supra* note 53.

[89] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 312 (N.J. 1987).

[90] *See, e.g.*, *Buckley*, 521 U.S. at 442. In *Buckley*, the United States Supreme Court noted that the plaintiff sought $950 per year in damages for thirty-six years, but that the average settlement for asbestos injury claims over a six- year period was $12,500. *Id*. Although this may or may not be an accurate cost comparison (Were the damages Buckley sought truly representative of the diagnostic costs? Were settlements by the Center for Claims Resolution representative, or did they omit high-value claims that went to court?), it shows that it is far from certain that monitoring costs will always be less expensive than the expected cost of disease, at least in purely monetary terms.

[91] *See id.* at 442–43. Whether toxic tort defendants or insurers are in a better position to bear the costs of medical tests is far beyond the scope of this note, but it is worth noting that—assuming the tests are medically necessary and will happen either way—the cost of those tests is a given, and from a societal standpoint someone will have to pay the cost of those tests. The only question is who: the victim, the wrongdoer, or an insurer?

about the potentially devastating financial impact medical monitoring cases could have on defendants.[92] It can also be hard to decide how to structure payment of medical monitoring damages; the successful plaintiff might not spend a lump sum payment on medical procedures, but an award of regular payments would require burdensome judicial supervision.[93]

[24] Finally, medical monitoring damages raise claim preclusion issues.[94] Claim preclusion prevents a plaintiff from suing a defendant twice over the same transaction or occurrence.[95] This is a problem when medical monitoring costs have been awarded, because a later suit for the disease would be based on the same occurrence as the medical monitoring suit.[96] A strict interpretation of claim preclusion would bar the second suit,[97] forcing the potential plaintiff to choose between compensation for preventive monitoring or compensation for the disease should it develop.[98]

---

[92] *See, e.g.*, Wood v. Wyeth-Ayerst Labs., 82 S.W.3d 849, 857 (Ky. 2002) (noting that requiring defendants to pay large medical monitoring judgments would impair their "ability to fully compensate victims who emerge years later with actual injuries that require immediate attention."); Henderson & Twerski, *supra* note 79, at 844; Hopp, *supra* note 63, at 439.

[93] *See Buckley*, 521 U.S. at 440–41 (noting the different ways medical monitoring payouts have been handled by courts, and discussing policy concerns about lump-sum payments).

[94] *See Wood*, 82 S.W.3d at 858–59; *see also* Tamara Jeanne Dodge, *Raging Hormones?: The Legal Obstacles and Policy Ramifications to Allowing Medical Monitoring Remedies in Hormone Replacement Therapy Suits*, 21 WIS. WOMEN'S L.J. 263, 287–88 (2006).

[95] *Wood*, 82 S.W.3d at 858.

[96] *See* Dodge, *supra* note 94, at 287.

[97] *See Wood* 82 S.W.3d at 858–59; Christine H. Kim, Note, *Piercing the Veil of Toxic Ignorance: Judicial Creation of Scientific Research*, 15 N.Y.U. ENVTL. L.J. 540, 573–74 (2007).

[98] *See, e.g.*, Miranda v. Shell Oil Co., 26 Cal. Rptr. 2d 655, 659–60 (Ct. App. 1993) (allowing medical monitoring costs but refusing to treat them as a distinct cause of action and discussing the potential problem this could create for the plaintiff if disease actually were to develop). The decision would be particularly hard because a toxic tort victim

Some courts, finding this forced choice to be inequitable, have endorsed claim- splitting in medical monitoring cases.[99] Because many states have rejected medical monitoring damages altogether and not all states that allow such claims have had to face the issue, claim preclusion in medical monitoring cases remains largely an unsettled question.[100]

[25] These concerns show why a large number of states have rejected medical monitoring as a cause of action, and why many of those that recognize medical monitoring claims either require present physical symptoms or view medical monitoring costs solely as a measure of damages.[101] Analysis of medical monitoring claims requires balancing conflicting policy benefits and costs; thus, it is an area in which courts are split.

---

could be medically better off getting preventive medical procedures but financially better off with compensation for the disease. *Id.* at 660.

[99] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 300 (N.J. 1987); Eagle-Picher Indus. v. Cox, 481 So. 2d 517, 521 (Fla. Dist. Ct. App. 1985).

[100] *See, e.g.*, Arch v. Am. Tobacco Co., 175 F.R.D. 469, 480 (E.D. Pa. 1997) (finding that under Pennsylvania law a claim for medical monitoring damages would not "theoretically" preclude a later claim should a disease develop); Pankaj Venugopal, *The Class Certification of Medical Monitoring Claims*, 102 COLUM. L. REV. 1659, 1674–78 (2002) (discussing claim preclusion for medical monitoring claims, and noting that "the case law is sparse," but speculating that courts that allow medical monitoring without present physical injury would probably allow later claims for physical injuries). Some authors cite this uncertainty as reason to reject medical monitoring damages altogether. *See, e.g.*, Dodge, *supra* note 94, at 288 (arguing that a court's position on the claim preclusion question is unforeseeable until it has met the issue, and thus it is poor policy to allow medical monitoring damages knowing that a claim for later injury might be precluded).

[101] *See* Dodge, *supra* note 94, at 287.

III. COMPARING MEDICAL MONITORING CLAIMS TO CLAIMS RESULTING FROM DATA LOSS

A. EXAMINING THE ANALOGY

[26] Data loss shares a number of features with toxic torts. Both involve claims resulting from exposure that may, over time, develop into serious and costly harms.[102] Whether the plaintiff is exposed to toxins or her data is exposed to others, the future harm of the exposure is expected to be much worse than any current harm.[103] In both cases, causation can be difficult to prove because of distance in time between the exposure and harm, and because there are multiple possible causes.[104] Physical harm is not a factor in data loss cases and is not always present in medical monitoring cases.[105] With both toxins and data loss, procedures may exist that can detect or mitigate the progress of the future harm.[106]

[27] Despite these similarities, several differences exist. The most obvious difference is that toxic tort claims involve physical injury, but data loss claims do not.[107] Even in toxic tort cases without present

[102] *See* Vincent R. Johnson, *Data Security and Tort Liability*, 11 No. 7 J. INTERNET L. 22, 29–30 (2008).

[103] *See generally Ayers*, 525 A.2d 287.

[104] *See id.* at 301 (discussing the difficulty of proving causation in toxic tort cases); Erin Dowe, *Frustration Station: Attempting to Control Your Credit*, 16 GEO. MASON U. CIV. RTS. L.J. 359, 362–63 (2006) (noting that the remoteness of identity fraud makes perpetrators hard to catch); *see also* discussion *supra* notes 21, 61.

[105] *See, e.g.*, Wood v. Wyeth-Ayerst Labs., 82 S.W.3d 849, 851 (Ky. 2002) (rejecting a medical monitoring claim from a plaintiff who alleged exposure to a drug but no physical harm); *Ayers*, 525 A.2d at 312–13 (allowing medical monitoring damages to plaintiffs who were exposed to water contaminated by the defendant, but who had not yet developed physical symptoms).

[106] *See* Johnson, *supra* note 102, at 29.

[107] *See id.*

physical injury, any future harm is medical.[108] Despite the stress resulting from identity fraud,[109] harms from data loss are almost entirely economic.[110] Because of the important governmental interest in public health and the irreversible nature of many illnesses, courts give medical harms greater consideration than harms that can be fully repaid with money.[111]

[28] Some differences involve the way future harms develop. For example, the time frames are different: although compromised data may not be misused for years, toxins can take decades to develop into disease.[112] And the reasons for the delayed harm are also different. Toxins take time to develop into disease because they affect the body gradually.[113] But the time between data loss and data misuse is mere delay. Harm from

---

[108] *See id.*

[109] *See* Kahle v. Litton Loan Servicing, 486 F.Supp. 2d 705, 712 (S.D. Ohio 2007) (noting "findings that identity theft results in more than purely pecuniary damages, including psychological or emotional distress").

[110] *But see* PAM DIXON, WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU 5 (2006), http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf. (discussing an exception to this general rule: medical identity fraud, where an imposter uses another's identifying information to get medical care). This form of fraud can be life threatening when bad information in a victim's medical records results in incorrect treatments. *Id.* at 6.

[111] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 311 (N.J. 1987).

[112] *See* Greenville v. W.R. Grace & Co., 827 F.2d 975, 978 (4th Cir. 1987) (noting that asbestos-related diseases "may not develop until decades after exposure"); Miranda v. Shell Oil Co., 26 Cal. Rptr. 2d 655, 659–60 (Ct. App. 1993) (discussing claims that might be precluded when "disease actually develops, years, perhaps decades" into the future); CASTLEMAN, *supra* note 61, at 91.

[113] *Miranda*, 26 Cal. Rptr.2d at 659. Indeed, some time delay is usually necessary for a toxic exposure to turn into a disease. Compromised data can be sued as soon as it is obtained, and some forms of data (such as credit card numbers) are more useful to the thief immediately after being stolen. *See id.*

data loss also requires an intervening third-party action.[114] The data alone does no harm until a third party uses it, but toxins produce disease on their own.[115]

[29] There is also a difference in general acceptance of the different remedial measures. Doctors, patients, and courts all recognize the importance of early diagnosis and treatment of diseases like cancer.[116] The usefulness of data-loss response measures is far less certain.[117] Medical tests are also individually prescribed by doctors according to their patients' particular needs. Credit monitoring, however, is a standardized product selected by the consumer without any professional evaluation of its usefulness.[118]

[30] The nature of exposure is also different. In toxic tort cases, a substance is released into the air or water, or is present in an environment where people are exposed to it.[119] Any number of people could potentially find themselves exposed at varying levels.[120] Data loss, however, is

[114] *See* Key v. DSW, Inc., 454 F.Supp. 2d 684, 691 (S.D. Ohio 2006). There is an exception to this general rule: a data compromise that makes the data public may create privacy issues. *Cf. id.* Imagine, for example, that a photo processing company accidentally posts someone's explicit pictures on the Internet. In that case, no action of a third party was required to create a harm. But privacy claims for data loss are different from the negligence claims contemplated by monitoring claims, and fall outside the scope of this note.

[115] *Cf. Ayers*, 525 A.2d at 299–300.

[116] *See id.* at 311.

[117] *See* discussion *infra* Part V.A.

[118] *See, e.g.*, *How is LifeLock Different From a Credit Monitoring System?*, http://www.lifelock.com/lifelock-for-people/how-we-do-it/how-is-lifelock-different-from-a-credit-monitoring-system (last visited Oct. 5, 2009).

[119] *See, e.g.*, D. Alan Rudlin & Christopher R. Graham, *Toxic Torts: A Primer*, 17 NAT. RESOURCES & ENV'T 210, 210 (2003).

[120] *See* Metro-N. Commuter R.R. Co. v. Buckley, 521 U.S. 424, 442 (1997).

comparatively well-defined and binary. Either a person's data is among a set of lost records or it is not.[121]

[31] Although it does not pose the same line-drawing problem inherent in exposure to toxins, data loss has a similar problem: it is unknown whether compromised data will actually be misused. Thus, some courts have imported the "exposure" question into data loss cases by requiring plaintiffs to show that their data was either (a) acquired or (b) misused by a third party, as opposed to merely lost.[122] This requirement is a little like the present-physical-injury element some courts require for medical monitoring recovery[123] and serves a similar purpose of rejecting plaintiffs whose injuries are too speculative.[124]

[32] The analogy is flawed. But do those flaws weigh in favor of accepting data loss monitoring, or against it? Factors are mixed. While data loss claims obviously lack the compelling public health justification, they are less prone to the exposure questions and infinite classes of plaintiffs in medical monitoring claims. The analogy alone is not enough to justify allowing or denying data loss monitoring claims. A full analysis

[121] If the data collector does not know which records were compromised, it should know what records it had, or at least all the possible records it had.

[122] *See, e.g.*, Stollenwerk v. Tri-West Health Care Alliance, 254 Fed. Appx. 664, 666 (9th Cir. 2007) (rejecting a claim for credit monitoring, arising out of stolen computer equipment, where the plaintiffs "offered no evidence the thieves had any interest in their personal information, rather than just the hardware."); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018 (D. Minn. 2006) (rejecting a credit monitoring claim because the plaintiffs had not shown that their data was accessed); Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *6 (D. Minn. Feb. 7, 2006) (rejecting a claim where the plaintiff "failed to present evidence that his personal data was targeted or accessed" by the people who stole a laptop with the plaintiff's data).

[123] *See supra* notes 54–56 and accompanying text.

[124] *See* Giordano v. Wachovia Secs., L.L.C., No. 06-476, 2006 WL 2177036, at *4 (D. N.J. July 31, 2006) (holding that the injuries plaintiff claimed were "speculative and hypothetical" because she could not show that data lost in the mail had actually been misused).

must look beyond the analogy and consider the policies behind these claims.

B. MOVING BEYOND THE ANALOGY: POLICY ARGUMENTS FOR AND AGAINST DATA LOSS CLAIMS

[33] Part II.B discussed medical monitoring claims' benefits and problems. The primary justifications for granting medical monitoring claims are interests in public health, deterrence, equity, and cost savings.[125] These claims, however, also suffer a number of problems, including the uncertainty of future harm, the difficulty in determining when there has been "exposure" absent present physical injury, potential health risks of monitoring procedures, the difficulty of determining how much an exposure has increased any need for prudent medical testing, the costs of monitoring compared to the disease, the cost burden on the defendant, and claim preclusion issues.[126]

[34] Not all of the benefits and problems associated with medical monitoring apply in data loss situations. Most notably, data loss claims lack a public health benefit.[127] But data loss claims also lack any public health danger because data monitoring, unlike many medical monitoring procedures, poses no health risk.[128] The lack of a public health danger is significant. In some jurisdictions, the lack of physical harm, whether immediate or occurring in the future, precludes inquiry into recovery for mitigation measures.[129] As a consequence, jurisdictions that refuse to entertain "novel" tort theories and insist that negligence is available only

[125] *See* discussion *supra* Part II.B.2.

[126] *See* discussion *supra* Part II.B.3.

[127] *See* Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. 223, 240–41 (2008).

[128] *See* discussion *supra* note 83 and accompanying text.

[129] *See* discussion *supra* Part II.B.1 and accompanying notes.

for injury to persons or property are unlikely to look past traditional tort principles in consideration of other justifications for data monitoring.[130]

[35] But there are other justifications for data monitoring claims. Remedial measures that allow data loss victims to mitigate the future cost, hassle, waste of time, and stress of responding to the misuse of data should be available if cost-effective.[131] Allowing plaintiffs to recover damages for reasonably necessary remedial measures would deter mishandling of data and require that the party responsible for losing the data pay the cost of those measures.[132] The justifications of deterrence, equity, and cost apply as much to data loss as they do in cases of physical harm.[133] The avoidable-consequences justifications may be even stronger in non-medical cases because the remedial measures do not require the plaintiff to submit to potentially dangerous medical procedures.[134]

[36] Many of the problems with medical monitoring also apply to data loss. These problems often involve determining when remedial measures are reasonably necessary.[135] The factors used in determining whether

---

[130] *See generally* Chandler, *supra* note 127, at 235–45 (discussing the difficulties plaintiffs face in showing actual harm and causation).

[131] *See id.* at 229–30, 242.

[132] 2007 GAO Report, *supra* note 15, at 6.

[133] *See* Chandler, *supra* note 127, at 242. Note that recovery for plaintiffs must come from negligence or strict liability unless a brand new tort cause of action is created. *See id*. at 230. Data loss plaintiffs usually lack any contractual privity with data handlers, leaving the plaintiffs without contract law remedies. *See id.* at 248–50. Additionally, because the United States treats data as property of the data collector, not the data subject, the subject has no remedies in property law. *See id.* As to statutory causes of action, no statute yet gives a private cause of action for recovering the costs of reasonably prudent measures taken in response to data loss.

[134] *See* RESTATEMENT (SECOND) OF TORTS § 918 cmt. e (1979) (commenting that it may not be unreasonable for someone to refuse to undergo medical procedures to avoid loss); STEIN, *supra* note 69 § 18:4.

[135] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 311 (N.J. 1987).

remedial measures are reasonably necessary include the likelihood of future harm, whether a plaintiff (or her data) has been exposed, how much of the risk of future harm comes from the exposure instead of from other sources, and the cost-effectiveness of remedial measures.[136] Courts denying credit monitoring have implicitly recognized these factors in cases where plaintiffs failed to show that credit monitoring was reasonably necessary.[137]

[37] Although data monitoring, like medical monitoring, may impose a heavy burden on defendants, data monitoring is essentially a loss-prevention measure. If monitoring is effective, the defendant pays less for the monitoring then it would have paid to compensate future loss.[138]

---

[136] *See* discussion, *infra* note 137.

[137] *See, e.g.*, Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873, 877 (E.D. La. 2008) (finding no cognizable losses from lost backup tapes where no evidence was offered that any data on those tapes was accessed); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712–13 (S.D. Ohio 2007) (rejecting claims by a plaintiff who sought the cost of credit monitoring after hard drives were stolen, but could not show that the data on those hard drives was the target of theft, and where there was no evidence that any unauthorized person was able to access the data on those drives); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021, 1021 n.3 (D. Minn. 2006) (rejecting credit monitoring damages based on a stolen laptop computer because the plaintiffs had not shown a present or "reasonably certain" future injury or any intent to misuse their lost information); Giordano v. Wachovia Secs., L.L.C., No. 06-476, 2006 WL 2177036, at *4 (D. N.J. July 31, 2006) (rejecting a claim for credit monitoring after a printout containing the plaintiff's social security number was lost in the mail). In each of these cases, there was no evidence that a third party had accessed the lost data. Lost laptop and lost media cases in particular seem doomed to failure. *But see* Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D. La. 2007). In *Ponder*, there was evidence that personal information of 17,000 current and former Pfizer employees was actually accessed and downloaded off of an employee's laptop computer. *Id*. at 794. The court still rejected the claim for credit monitoring because that data had not been misused and because there had been no physical injury. *Id.* at 796–98.

[138] *See* Johnson, *supra* note 102, at 29. If data handlers would save money by paying for paying for monitoring costs instead of waiting and paying for latent harms, why would they ever avoid paying for monitoring? Presumably, one does not have to resort to legal remedies to persuade companies to save money. Indeed, companies are already paying for a limited amount of monitoring in the form of free credit monitoring to data breach victims. *See* 2007 GAO Report, *supra* note 15 at 35. But there are reasons an

Furthermore, the burden of data monitoring on the defendant is limited because the class of potential data monitoring plaintiffs consists only of those whose data was mishandled.[139] For example, if an intruder were to access a company's database of one thousand customers, only those one thousand customers could have claims. A data handler could therefore prospectively limit its exposure to litigation not only by handling data carefully, but also by limiting the number of people about whom it collects data.[140] The burden on data handlers could be further reduced by requiring plaintiffs to allege actual disclosure to a third party (as opposed to mere loss) and by requiring proof that the remedial measures are reasonably necessary.[141]

[38] Claim preclusion is an issue for both data loss claims and medical monitoring claims, requiring potential plaintiffs to choose whether to seek immediate recovery for remedial measures or wait and preserve a claim for a later loss.[142] Although the choice would be difficult, it is at least a choice the data loss victim otherwise would not have had. One author has suggested making this tradeoff explicit by limiting the liability of breached organizations to the cost of reasonably necessary steps to prevent identity

organization might not voluntarily pay for extended monitoring, even when it would save money. Organizations cannot predict the future, so do not know when present monitoring would be less expensive than latent harms. They might also prefer to risk possible future lawsuits rather than make definite payments in the present—especially if those potential lawsuits are far enough in the future that plaintiffs would have trouble proving causation. *See* Chandler, *supra* note 127, at 235–38 (discussing the difficulties plaintiffs face in proving causation in data fraud cases).

[139] *See* Chandler, supra note 127, at 242.

[140] *See id.*

[141] Stollenwerk v. Tri-W. Health Care Alliance, 254 Fed. Appx. 664, 666 (9th Cir. 2007); *see* Ayers v. Twp. of Jackson, 525 A.2d 287, 312 (N.J. 1987).; Johnson, *supra* note 102, at 29.

[142] *See* Chandler, *supra* note 127, at 238–44.

fraud.[143] But such a liability cap would only make sense if these measures were actually effective.

IV. CRITERIA FOR AWARDING NON-MEDICAL MONITORING DAMAGES

A. AWARDING DAMAGES BASED ON REASONABLE NECESSITY

[39] Even though the analogy between medical monitoring and data monitoring is flawed, non-medical monitoring may still be justified in certain cases. Adapting the criteria used in medical monitoring cases to non-medical situations gives a similar test.[144] A plaintiff should be allowed recovery when (1) there is a precipitating event, (2) that event resulted from the defendant's negligence, (3) the event increased the plaintiff's risk of future harm, (4) there exist preventive remedial measures, and (5) those measures are reasonably necessary.[145]

[40] This model relies on standard negligence theory. It does not create a new cause of action, but instead recognizes reasonably necessary costs as a measure of negligence damages and, therefore, requires proof for all standard elements of negligence, including cause-in-fact and proximate cause.[146] The model also requires that the plaintiff not only have a risk of future harm, but an *increased* risk, and that the increase have been caused by the breach.[147]

---

[143] *See* Johnson, *supra* note 102, at 29–30.

[144] *See* discussion *supra* Part II.B.1 and accompanying notes.

[145] *Cf.* Schwartz, *supra* note 83, at 356–57. Put in data breach terms, this would require that (1) the plaintiff's data was exposed in a breach; (2) the defendant negligently caused that breach; (3) the data breach created an increased risk that the plaintiff will suffer future fraud or other harm; (4) a way exists to reduce or eliminate that risk, and (5) the defendant's negligence made those measures reasonably necessary. *See* discussion *supra* Part II.B.1 and accompanying notes.

[146] *See* Chandler, *supra* note 127, at 235–45 (discussing how courts have historically found against plaintiffs in data loss cases because of a failure to show actual harm or causation).

[147] *See supra* notes 48–53 and accompanying text.

[41] The central feature of this model is that it allows recovery for remedial measures that are reasonably necessary. This reflects the approach followed in *Ayers*, which allowed costs reasonably incurred by the plaintiff as legitimate measures of harm stemming from a defendant's actions.[148] The model also recognizes that under the doctrine of avoidable consequences, plaintiffs are expected to take reasonably necessary remedial measures.[149]

[42] But when are remedial measures reasonably necessary? One approach would be to apply the same reasonable person standard that is usually employed in determining what is objectively "reasonable."[150] This is the approach of the avoidable consequences doctrine, and a first and necessary step to keep the model in conformity with existing tests.[151] But a test for the reasonable necessity of remedial measures should go beyond a mere reasonable-person inquiry. Certain situations may increase confidence that data monitoring costs are reasonably necessary.[152] For example, remedial measures may be more likely to be reasonably necessary when the plaintiff's data was actually exposed to a third-party, creating an increased risk that the plaintiff will suffer future fraud. Remedial measures might also be considered more likely to be necessary when those measures are cost-effective in the aggregate—i.e., when the expected total costs of the breach when remedial measures are used are much lower than the expected costs without remedial measures.[153]

---

[148] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 311 (N.J. 1987).

[149] *See* discussion *infra* Part IV.B and accompanying notes.

[150] *See* RESTATEMENT (SECOND) OF TORTS § 918 cmt. c ("[t]he factors determining whether an injured person has used care to avert the consequences of a tort are in general the same as those that determine whether a person has been guilty of negligent conduct").

[151] *See id.*; STEIN, *supra* note 69, § 18:1.

[152] *See* STEIN, *supra* note 69, § 18:1.

[153] *See* discussion *supra* note 137 and accompanying text.

[43] A federal district court in New York suggested some possible minimum criteria for establishing "exposure" of data.[154] Trying to apply New York law in an area where New York had not yet spoken, the court held that New York would likely require a plaintiff to show a "demonstrable basis for a serious concern over misuse" of data on a lost laptop.[155] The court listed several factors that might be used to show such a basis: (1) lack of password protection, (2) intent and ability by the laptop thief to access the data, or (3) actual misuse of information that was on the hard drive.[156]

[44] The reasonable necessity model is consistent with cases that have both allowed[157] and rejected medical monitoring claims.[158] In *Stollenwerk*, for example, the court rejected the plaintiff's claim because she had not

[154] *See* Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281–82 (S.D.N.Y. 2008).

[155] *Id.*

[156] *Id*. The misused information would not have to be the plaintiff's information; concern over misuse could also be established by showing that someone else's data from the same stolen hard drive had been misused. *See id.*

[157] *See* Ayers v. Twp. of Jackson, 525 A.2d 287, 312 (N.J. 1987) (noting that it would be inequitable to force someone wrongfully exposed to toxic chemicals "to have to pay his own expenses when medical intervention is clearly reasonable and necessary.").

[158] One of the exceptions seems to be the result of confusion on the part of the court. *See generally* Giordano v. Wachovia Secs., L.L.C., No. 06-476, 2006 WL 2177036 (D. N.J. July 31, 2006). The court in *Giordano* rejected an analogy between credit monitoring and medical monitoring because the latter requires an actual exposure to a toxin, not a mere potential exposure. *Id.* at *3 n.4. It held that because the plaintiff had merely alleged potential identity fraud, not actual fraud, she had not shown "exposure." *Id*. This analysis misinterprets the analogy. Identity theft was the future harm that credit monitoring was meant to prevent. Asking the plaintiff to show actual fraud before seeking credit monitoring is like asking someone exposed to asbestos to prove that she has cancer before allowing her to seek the cost of tests to detect cancer. A more appropriate analysis would have required the plaintiff to show that the data breach actually exposed her data to a third party.

shown that credit monitoring was reasonably necessary.[159] The model's requirement that a plaintiff show data exposure also fits several cases that refused to allow credit monitoring for lack of data misuse.[160] Of course, not all courts would follow the model, especially those that require present physical harm for medical monitoring claims or those that do not allow negligence recovery for economic harms. But for those courts willing to look to non-physical forms of negligence harm, the reasonable necessity model fits.

B. STANDING AND THE DOCTRINE OF AVOIDABLE CONSEQUENCES

[45] The doctrine of avoidable consequences provides another reason to allow recovery of the costs of reasonably necessary remedial measures. The doctrine holds that a tort plaintiff may not recover damages for any harm she could reasonably have avoided.[161] This doctrine, however, may

[159] Stollenwerk v. Tri-W. Health Care Alliance, 254 F. Appx 664, 666–67 (9th Cir. 2007). The court held that the plaintiff had made "no showing that a *normally prudent* person in these circumstances" would have obtained "premium credit monitoring," and that the plaintiff's expert testimony was "entirely too conclusory to establish that a *reasonable person* faced with Stollenwerk's level of risk of identity theft would incur significant monitoring costs." *Id.* (emphasis added).

[160] *See, e.g.*, Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281–82 (S.D.N.Y. 2008) (rejecting a claim for credit monitoring where the plaintiff could not show that there was a "rational basis" to believe that data on a stolen laptop would be misused); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 710–11 (S.D. Ohio 2007) (rejecting credit monitoring where there was no evidence that information from a stolen hard drive had been accessed by unauthorized individuals or that it would be used for unlawful purposes if accessed); *see also* discussion *supra* note 137.

[161] *See* RESTATEMENT (SECOND) OF TORTS § 918 (1979). The standard of behavior for the avoidable consequences doctrine is the same as for negligence: reasonable behavior under all the circumstances. *Id.* § 918 cmt. c; *see also* STEIN, *supra* note 69 § 18:4. The plaintiff is not required to calculate all the probabilities nor is he "bound at his or her peril to know the best thing to do." *Id.* § 18:1. But the likelihood that remedial measures will be successful is a factor in considering whether a plaintiff is expected to take remedial measures. RESTATEMENT (SECOND) OF TORTS § 918 cmt. e.

conflict with the constitutional requirement of standing.[162] The tension arises when inexpensive remedial measures may prevent large, unlikely losses. For example, suppose one could spend $100 to avoid a one percent chance of losing $1,000,000. Spending the $100 would be rational. The expected loss from a one percent chance of losing $1,000,000 is $10,000—one hundred times the cost of avoiding the loss.[163] But a court may say that a one-percent probability of loss is too unlikely to establish standing, regardless of the amount of potential loss.

[46] In monitoring cases, the doctrines of avoidable consequences and standing have conflicting goals. The doctrine of avoidable consequences reflects the importance of taking reasonable measures to avoid loss; the amount of potential loss figures into the reasonableness analysis.[164] But standing is meant to bar speculative claims–it depends on how likely a loss is, not the potential size of the loss.[165] The result in cases with a small probability of a large loss is that the plaintiff is left without recovery. The avoidable consequences doctrine prevents a plaintiff from recovering the million-dollar loss that could reasonably have been mitigated, but lack of standing bars any claims for the mitigation.[166]

---

[162] *See Ayers*, 525 A.2d at 310–11 (noting that under the avoidable consequences rule, a plaintiff "is required to submit to treatment that is medically advisable; failure to do so may bar future recovery for a condition he could thereby have alleviated or avoided."); *see also* Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (discussing the required showings to establish standing).

[163] People make reasonable decisions that do not necessarily match this simple example of a rational choice, so a reasonable person might not actually make this choice depending on that person's preferences, risk tolerance, and other factors. *See generally* Bruce Chapman, *The Rational and The Reasonable: Social Choice Theory and Adjudication*, 61 U. CHI. L. REV. 41 (1994).

[164] *See* STEIN, supra note 69 § 18:1 (noting that the doctrine of avoidable consequences is applied based on what is "reasonable under all of the circumstances.").

[165] *See Lujan*, 504 U.S. at 561 (reiterating that constitutional standing requires an injury that is likely, not speculative).

[166] *See* Chapman, *supra* note 163, 88–89; STEIN, *supra* note 69, § 18:1.

[47] The key to resolving this conflict lies in understanding the harm in monitoring cases. Many courts that have found a lack of standing have focused on the likelihood of eventual loss–the one percent probability.[167] But when remedial measures are reasonably necessary, the harm is the necessity of expenses the plaintiff would not otherwise have incurred, not whatever future injury would have resulted had the measures not been taken.[168] A reasonable-necessity standard recognizes standing to seek compensation for those plaintiffs that have taken the remedial measures the doctrine of avoidable consequences expects.[169]

C. COST ANALYSIS OF REMEDIAL MEASURES FOR LATENT HARM

[48] Recovery for post-breach remedial measures is likely to be reasonably necessary only if the measures save money—if recovery for these measures would be less expensive than waiting for the latent harm to mature.[170] One way to determine this is by comparing the estimated expected costs of a data breach with and without remedial measures. If the expected cost of a data breach with remedial measures is significantly lower than the expected cost without them, those measures could be considered reasonably necessary. Conversely, if the expected costs do not significantly decline when remedial measures are taken, it is unlikely that those measures would be found to be reasonably necessary.[171]

---

[167] *See* discussion *supra* note 28 and accompanying text.

[168] *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 851 (3d Cir. 1990) ("the appropriate inquiry is not whether it is reasonably probable that plaintiffs will suffer harm in the future, but rather whether medical monitoring is, to a reasonable degree of medical certainty, necessary in order to diagnose properly the warning signs of disease.").

[169] *See* RESTATEMENT (SECOND) OF TORTS § 918 cmt. b (1979) (noting that when a plaintiff has failed to make substantial efforts to avert the consequences of a tort, damages are reduced to the amount of the expense that plaintiff should have taken).

[170] *See id.* § 918 cmt. h.

[171] Note that this simple comparison does not account for the cost to the system of litigating claims. Litigation would probably increase or become more complex with the field of potential plaintiffs opened to those who incurred reasonably necessary monitoring expenses. For remedial measures to be reasonably necessary, their cost

[49] The expected cost of latent harm without remedial measures for an individual victim is determined by the increase in probability of loss attributable to the event multiplied by the amount of that victim's loss.[172] Assuming a uniform probability of loss,[173] the total expected cost of a latent harm for all victims is equal to the product of (a) the increase in probability of loss attributable to the event, (b) the average loss, and (c) the number of victims affected.[174]

[50] The expected cost with remedial measures is slightly more complicated than the expected cost without them. In addition to the cost of the measures themselves, the calculation must include the cost of latent harms that still occur despite the remedial measures, independent of whether or not the plaintiffs can recover these latent harms.[175] The calculation must also include the risk that the remedial measures might do harm of their own. Thus, the expected cost of remedial measures is the sum of (a) the cost of the measures themselves, (b) the cost of residual latent harm, and (c) the risk of additional harm from the remedial measures themselves.

---

therefore should be significantly lower than the cost without them—i.e., anything near a break-even comparison should default to disallowing the remedial measures.

[172] *See* Philippe Mongin, *Expected Utility Theory*, *in* HANDBOOK OF ECONOMIC METHODOLOGY 171 (John B. Davis, D. Wade Hands & Uskali Mäki ed., Edward Elgar Publishing 1998).

[173] A uniform probability of loss would mean that each breach victim has the same probability of latent harm as each other victim.

[174] The appropriate calculation is the expected cost for all victims because this more fully reflects the societal costs of a breach as well as the potential cost to a breached organization.

[175] When remedial measures are not one hundred percent effective at preventing the latent harm, some of that latent harm happens anyway. For example, assume a remedial measure successfully reduces the eventual loss by fifty percent. The total expected cost is the cost of providing remedial measures to all the victims, plus the fifty percent residual latent harm. To put this into numbers, suppose the cost of remedial measures is $100 per victim, the latent harm is $10,000 per victim, and the remedial measures are 50% effective with no harmful side effects. The expected cost per victim is $100 + 0.50($10,000) = $5100.

V. APPLYING THE REASONABLE NECESSITY MODEL TO DATA BREACHES

[51] As previously discussed, remedial measures are cost-effective when the aggregate expected loss with remedial measures is substantially lower than the aggregate expected loss without those measures.[176] The expected loss from identity fraud resulting from a data breach depends on three variables: the cost of identity fraud, the cost and effectiveness of measures designed to prevent or mitigate identity fraud, and the probability that a data breach will lead to identity fraud.[177] The remainder of this article uses available information on data breach and identity fraud to estimate whether data monitoring options are cost-effective and, thus, potentially reasonably necessary.[178]

A. COST OF IDENTITY FRAUD

[52] How much does identity fraud cost? It is a simple question with a complex answer. The total cost of identity fraud depends on the answers to other questions. Does "cost" include time and effort spent responding to a fraud, or only financial loss? Is the measure of "cost" the out-of-pocket expense to the identity fraud victim, the value of goods stolen, or overall systematic cost? The cost of identity fraud also depends on the type of fraud. The harms, and therefore, the costs, differ depending on

[176] *See* discussion *supra* Part IV.C.

[177] *See id.*

[178] As discussed more fully below, much of the available data is contradictory or of suspect quality. In some cases the only redeeming feature is that the data is (probably) better than nothing. All is not lost, however. Evaluating the viability of data monitoring damages only requires determining whether the expected cost of a breach with remedial measures is substantially greater than the expected cost without them. If the inequality is so substantial that any margin of error in the data is irrelevant, that is still a useful result. Precision only matters if the inequality is close—which would not clearly establish the substantial economic benefit required to show reasonable necessity. In short, even with faulty data, any result other than one that overwhelmingly shows cost-effectiveness argues against allowing data monitoring claims.

whether the fraud is on a new account, existing account, or is non-financial.

[53] Experts generally distinguish between three forms of identity fraud: new account fraud, existing account fraud, and non-financial fraud.[179] New account fraud happens when someone uses a victim's personal information to create a new account, such as a loan, in the victim's name.[180] Existing account fraud occurs when one of a victim's accounts, such as a credit card or checking account, is used without authorization.[181] Non-financial fraud can result from other uses of someone's identity, such as medical identity fraud, where someone gives false information to get medical care; criminal identity fraud, where a suspect or arrestee impersonates someone else; or employment identity

[179] *See, e.g.*, SYNOVATE, FED. TRADE COMM'N: 2006 IDENTITY THEFT SURVEY REPORT 12 (2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf [hereinafter 2006 FTC Survey]; Schreft, *supra* note 12, at 7; Towle, *supra* note 12, at 242–47.

[180] *See, e.g.*, 2007 GAO Report, *supra* note 15, at 2.

[181] *See id*. Some sources refer to this as "account takeover" or "account hijacking." *See, e.g.*, FED. DEPOSIT INS. CORP., PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT 4–6 (2004), www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf. A few experts further distinguish between credit-card fraud and other forms of existing account fraud. *See* Katrina Baum, *Identity Theft, 2005*, BUREAU OF JUSTICE OF JUSTICE STATISTICS SPECIAL REPORT, Nov. 2007, at 1, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/it05.pdf [hereinafter 2005 BJS Survey]. Federal law limits consumer liability for unauthorized credit and debit card use. *See* 15 U.S.C. §§ 1643(a)(1)(B), 1693(g)(a) (2006); 12 C.F.R. §§ 226.12(b), 205.6(b) (2009). Visa and MasterCard have also instituted zero-liability policies, further reducing consumer liability for credit card fraud. *See* Douglas Akers et al., *Overview of Recent Developments in the Credit Card Industry*, 17 No. 3 FDIC BANKING REV. 23, 32 n.46 (2005), *available at* www.fdic.gov/bank/analytical/banking/2005nov/article2.pdf. These laws and policies make credit card fraud a very low-cost form of fraud for the consumer, and some studies therefore distinguish it from other forms of existing-account fraud.

fraud, where the perpetrator uses someone else's identity to gain employment.[182]

[54] Several studies have attempted to measure identity fraud costs.[183] The Federal Trade Commission (FTC) began collecting consumer identity fraud complaints in 1999,[184] and has published reports on its data since 2000.[185] It also commissioned surveys in 2003[186] and 2007.[187] The Bureau of Justice Statistics of the Department of Justice (BJS) has also surveyed identity fraud victims.[188] Non-government surveys include those by the

[182] *See* Jim Collins, *Identity Theft: The Pros and Cons of Identity Scoring vs. Credit Monitoring*, YOUNG MONEY, July 8, 2008, http://www.youngmoney.com/credit_reports/281.

[183] *See, e.g.*, FED. TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JAN.–DEC. 2007 (2008), http://www.ftc.gov/opa/2008/02/fraud.pdf [hereinafter 2008 FTC Complaint Data]; IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 2007 (2008), http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf [hereinafter 2007 ITRC Survey]; JAVELIN STRATEGY & RESEARCH, 2009 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION (2009), http://www.idsafety.net/901.R_IdentityFraudSurveyConsumerReport.pdf [hereinafter 2009 Javelin Survey]; 2005 BJS Survey, *supra* note 181; CTR. FOR IDENTITY MGMT. & INFO. PROT., IDENTITY FRAUD TRENDS AND PATTERNS: BUILDING A DATA-BASED FOUNDATION FOR PROACTIVE ENFORCEMENT (2007), http://www.utica.edu/academic/institutes/ecil/publications/media/cimip_id_theft_study_oct22_noon.pdf [hereinafter 2007 CIMIP Report]; 2006 FTC Survey, *supra* note 179.

[184] *See* FED. TRADE COMM'N, OVERVIEW OF THE IDENTITY THEFT PROGRAM (2003), http://www.ftc.gov/os/2003/09/timelinereport.pdf.

[185] *See* FED. TRADE COMM'N, NATIONAL DATA, http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html (last visited Oct. 5, 2009).

[186] *See generally* 2006 FTC Survey, *supra* note 179.

[187] *See id.*

[188] *See generally* 2005 BJS Survey, *supra* note 181.

Identity Theft Resource Center (ITRC)[189] and Javelin Strategy & Research.[190]

[55] These studies vary widely in their methodologies.[191] Unsurprisingly, they also vary widely in their results. The Javelin and

[189] *See* 2007 ITRC Survey, *supra* note 183.

[190] *See* 2009 Javelin Survey, *supra* note 183; JAVELIN STRATEGY & RESEARCH, SYNDICATED REPORT BROCHURE, 2009 IDENTITY FRAUD SURVEY REPORT: IDENTITY FRAUD ON THE RISE, BUT COSTS PLUMMET AS PROTECTIONS INCREASE (2009), http://www.javelinstrategy.com/uploads/901.R_IdentityFraudSurveyBrochure.pdf; *see also* BBBOnline.org, New Research Shows Identity Fraud Growth is Contained and Consumers Have More Control than they Think, http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited Oct. 5, 2009). Javelin's optimism might be related to the fact that it is also consults for the financial services industry. *See* Eve Mitchell, *ID Theft Poses a Bigger Risk Offline*, PITTS. POST-GAZETTE, June 10, 2008, at A6, *available at* http://www.post-gazette.com/pg/08162/888660-28.stm; Javelin Strategy & Research, Clients, http://www.javelinstrategy.com/about/portfolio (last visited Oct. 5, 2009).

[191] The 2006 FTC survey used random-digit-dialing phone interviews of 4917 people. 2006 FTC Survey, *supra* note 179, at 3. Its statistics were based on the 559 people who reported "discovering the misuse of their personal information" since 2001. *Id.* at 17 n.4. The ITRC, by contrast, e-mailed its survey to 1031 identity fraud victims who had contacted the ITRC in the previous year. 2007 ITRC Survey, *supra* note 183, at 36. It received responses from 117 victims. *Id.* The ITRC claims a fourteen percent "response rate," based on the 817 people who it believed actually received a survey after 214 e-mails were returned as undeliverable. *Id.* This is more accurately termed a cooperation rate. *See* Am. Ass'n for Public Opinion Research, Standard Definitions: Final Dispositions of Case Codes and Outcome Rates for Surveys (2008), http://www.aapor.org/content/NavigationMenu/ResourcesforResearchers/StandardDefinitions/Standard_Definitions_07_08_Final.pdf. Note that the respondents in the ITRC survey self-selected twice: once in contacting the ITRC in the first place, and again in choosing to respond to the survey. *See* 2007 ITRC Survey, *supra* note 183, at 36. The Javelin study also used phone surveys, contacting 4,784 respondents, 482 of whom said they were identity fraud victims. 2009 Javelin Survey, *supra* note 183, at 18. The FTC's consumer complaint data was based on actual self-reported and unverified consumer complaints, not a survey. 2008 FTC Complaint Data, *supra* note 183, at 2. The BJS included identity fraud questions as a supplement to its National Crime Victimization Survey, which is conducted by the Census Bureau and surveys about 76,000 people. *See* 2005 BJS Survey, *supra* note 181, at 6; Michael Rand & Shannan Catalano, *Criminal*

ITRC surveys both reported measures of average[192] out-of-pocket[193] losses.[194] Javelin's survey found that fraud victims lost "almost $500" over all forms of identity fraud.[195] The ITRC reported average losses of $550 per victim for existing-account frauds and $1865 for new-account frauds.[196] All four surveys also reported total-loss[197] figures: $1620 (BJS),[198] $1882 (FTC),[199] $5555 (Javelin),[200] and $48,941.11 (ITRC)[201] per

Victimization, 2006, BUREAU OF JUSTICE STATISTICS BULLETIN, December 2007, at 7, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/cv06.pdf.

[192] Although median values more accurately represent the typical identity fraud victim's experience, average (mean) values are more relevant to the calculation of aggregate expected losses because of the relationship between averages and totals. But they are also more easily influenced by small numbers of outlier responses.

[193] Out-of-pocket losses include only unreimbursed expenses incurred by identity fraud victims. Goods and services that are stolen but which that the identity theft victim does not eventually pay for would not be included in out-of- pocket losses.

[194] *See* 2009 Javelin Survey, *supra* note 183, at 5, 20; 2007 ITRC Survey, *supra* note 183, at 3.

[195] 2009 Javelin Survey, *supra* note 183, at 5.

[196] 2007 ITRC Survey, *supra* note 183, at 17. The $1865 figure for new-account fraud was based on the responses of only forty-five people; ITRC did not reveal the number of people whose responses formed the basis of the $550 figure for existing accounts. *Id.*; *see also* discussion *supra* note 191 (noting the methodological flaws with the ITRC Survey).

[197] Total losses include the total value of goods and services stolen, not only victims' out-of-pocket expenses.

[198] 2005 BJS Survey, *supra* note 181, at 5. This number reflects a survey question that asked for the total dollar amount obtained ("[w]hat was the total dollar amount of the credit, loans, cash, services, and anything else the person obtained while misusing (the credit card account(s)/any existing accounts other than credit cards/personal information or new account(s))?"). *Id.* at 7.

[199] 2006 FTC Survey, *supra* note 179, at 8. The FTC survey also reported detailed median and percentile data broken down by identity fraud type (identifying as new account, existing account, and credit-card only), but only reported overall means. *Id.* at 5–8. The survey reported median out-of-pocket costs of $0 for existing-account fraud, and $40 for new account fraud. *Id.* at 5.

victim. The BJS survey further categorized total losses by type of fraud, reporting averages of $4850 for new-account frauds, $980 for existing-credit-card frauds, and $1220 for other existing-account frauds.[202]

[56] The surveys also varied widely in the amounts reportedly lost by victims. A survey of cases handled by the U.S. Secret Service reported actual loss figures that ranged from no loss in thirty-four cases to a thirteen-million dollar loss in one case.[203] The same survey reported that eighteen percent of defendants ordered to pay restitution were required to pay more than $100,000.[204] These numbers show how a few very high-

[200] *See* JAVELIN STRATEGY & RESEARCH, 2008 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 4 (2008), www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%20Version.pdf. The publicly available version of Javelin's 2008 survey did not report an average, but said that 8.1 million people were victimized by identity fraud for a total of $45 billion, equivalent to a $5555.00 average per-person loss. Note, however, that this is a per-person estimate, not a per-incident estimate, and does not factor in the possibility that the 8.1 million person figure includes each member of families (i.e., so that a family of four suffering one fraud incident would count as four people, not one incident). *See id.*

[201] 2007 ITRC Survey, *supra* note 183, at 18. This number reflects a $48,941.11 cost to businesses (survey respondents were asked "to total the charges on the fraudulent accounts in their name . . . based on how much money victims were billed by creditors, banks, and collection agencies, as well as other related costs"). *Id.* Note, however, that this number is based on the responses of only forty-eight people, and does not exclude six outliers who reported between $100,000 and $700,000 in total losses. *Id.; see also* discussion *supra* note 191 on the ITRC survey's methodological flaws.

[202] 2005 BJS Survey, *supra* note 181, at 5. The BJS survey categorized frauds as involving the "unauthorized use or attempted use of existing credit cards," "other existing accounts," or "personal information." *Id.* Because misuse of personal information is most closely associated with new-account fraud, the BJS results for "personal information" are included with new-account fraud data in this note. *See id.*

[203] 2007 CIMIP Report, *supra* note 183, at 26–27.

[204] *Id.* at 25.

value cases skew the overall averages.[205] The averages should, therefore, be considered very rough figures at best.

[57] What, then, is the cost of identity fraud? The answer is somewhere between "it depends" and "answer hazy, ask again later." Even within a particular type of fraud and measure of loss, different surveys—some with significant methodological flaws—give widely different results. For the purposes of analyzing data monitoring cost effectiveness, the best that can be done is to work with the numbers that are available while recognizing their problems.

B. PROBABILITY THAT A DATA BREACH WILL LEAD TO IDENTITY FRAUD

[58] If the cost of identity fraud is a complicated question, the probability that a data breach will lead to identity fraud is downright inscrutable. No study measures this probability.[206] A rudimentary calculation of the probability that a data breach will lead to identity fraud could be done by dividing (a) the number of identity fraud cases caused by data breach by (b) the total number of fraud-enabling records exposed in data breaches.[207] A proper calculation is not that simple, but even that level of estimation is difficult to do because the necessary data is flawed.[208]

---

[205] This does not imply that an arithmetic mean is the wrong measure for evaluating cost effectiveness of remedial measures. Aggregate cost savings depends on reducing total amount of losses, not on reducing losses for the most people. But these numbers do show how a few very costly fraud cases can dramatically shift an average.

[206] Estimates have been done for the rate of credit card misuse, but not for identity fraud more broadly. *See, e.g.*, Thomas M. Lenard & Paul H. Rubin, *Much Ado About Notification*, REGULATION, Spring 2006, at 44, 47.

[207] "Fraud-enabling" records would be records that contain data that can be used to perpetrate identity fraud.

[208] One complication involves time frames. What time period of data breaches and what time period of identity fraud cases should one compare? Data breaches release data that may be used years later for fraud, so simply comparing a year's worth of data breaches to the same year's number of identity frauds compares unrelated numbers. Data breaches are also reported according the year the breach was discovered, but a few breaches occur

[59] Part of the problem is that the different parts of the calculation are tracked using different units of measure, making direct comparison difficult. Identity fraud figures count people or households, but data breach statistics are tracked by number of records.[209] The number of records compromised in a data breach may not be the same as the number of people involved. For example, although a record may be a customer, it could also be a transaction or a credit card entry. Even if each record is a person, a database could have multiple entries for the same person.[210] Finally, some people may have been affected by multiple breaches; simply adding all records in all breach events would count these people multiple times.

[60] Another problem is data incompleteness. Many organizations have carefully studied the causes, sources, and amount of identity fraud,[211] but data breach numbers are far less certain. Most breach numbers are known only because state data breach notification laws require organizations to

over a long time before they are discovered. For example, hackers were able to steal credit card numbers from TJX over a seventeen-month period. *See* Mark Jewell, *Security Breach at TJX Believed to be Biggest Ever*, SAN JOSE MERCURY NEWS, Apr. 22, 2007, at 1E. The forty five million records affected are usually all counted for 2007, the year the problem was discovered. *See, e.g.*, Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 5, 2009) (including TJX in the list of 2007 data breaches). A year-by-year comparison also assumes that compromised data is either used for fraud or discarded at about the same rate as breached data becomes available. But another possibility exists: that breached data is accumulated in bulk then used over a period of time, like a windfall profit spent gradually. Such a pattern would require knowing not just the amount of compromised fraud-enabling data and the number of identity fraud over a seventeen-month period. *Cf.* Jewell, *supra*. This is not an easy problem.

[209] *See* Privacy Rights Clearinghouse, *supra* note 208. The Open Security Foundation maintains a database of announced data breaches, which includes the number of records affected by a breach—but that does not include unannounced breaches. *See* Open Security Foundation, http://opensecurityfoundation.org (last visited Oct. 5, 2009).

[210] These duplications can result from address changes, name changes, or different spellings, for example.

[211] *See, e.g.,* 2006 FTC Survey, *supra* note 179.

notify consumers when their data may have been compromised.[212] But not all states have these laws and not all of these laws require telling a law enforcement agency or the general public about a breach.[213] Some data breaches affect an unknown number of records, and therefore are not counted in breach totals.[214] Any count of lost data breach records, therefore, only includes the number of known cases.[215] The number of known data breaches—nearly 400 million records since 2000—is only a part of the total number of records affected.[216]

[61] Because of these issues, certain assumptions must be made when estimating the probability that a breach will lead to identity fraud. As mentioned above, data breach statistics measure records, not people, and understate the total number of records affected. Nevertheless, the following calculations use these statistics and assume that the underestimations and overestimations in these numbers cancel each other

[212] *See, e.g.*, CAL. CIV. CODE § 1798.29(a) (West 2008).

[213] *See* Jospeh Pereira, Jennifer Levitz, & Jeremy Singer-Vine, *Some Stores Quiet Over Card Breach*, WALL ST. J., Aug. 11, 2008, at B1 (reporting that four of the chains named as breach victims in FBI indictments of credit card thieves had never told their customers about the breaches); David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 No. 7 INTELL. PROP. & TECH. L.J. 5, 6 (2007) (noting that "a few" of the many state breach laws require reporting all breaches to state agencies).

[214] *See* Privacy Rights Clearinghouse, *supra* note 208 ("[f]or many of the breaches listed, the number of records is unknown.").

[215] Undetected breaches also go uncounted in this total. No one knows how many undetected breaches there are, but they do happen. The TJX breach, for example, operated for at least seventeen months before the company noticed. Jewell, *supra* note 208, at 1E. The breach at Heartland Payment Systems was also undetected for a few months. *See* Eric Dash & Brad Stone, *Big Breach in Card Data Raises Risk for Millions*, N.Y. TIMES, Jan. 21, 2009, at B4 (reporting that data thieves installed data-capturing software in May, but that that the breach was not discovered until late fall).

[216] *See* OSF Data Loss Database, http://datalossdb.org/download (last visited Oct. 5, 2009) [hereinafter OSF Database] (arranging breaches by date and adding the total number of breaches from 2000 through 2008).

out, or at least result in an overall underestimate.[217] The calculations also compare annualized data for years since 2005 when data is available.[218] This comparison assumes that breached data is used as it is obtained[219] and assumes a constant probability that breached data will be used for identity fraud (i.e., that this probability has not been increasing or decreasing over time).

[62] Under these assumptions, the basic calculations are straightforward. The first component is the number of records affected by data breach per year. According to the Open Security Foundation (OSF) data breach database, organizations announced breaches of about 354 million data records from 2005 through 2008—an average of roughly 88.5 million records per year.[220] Approximately 83.5 million records wereaffected in 2008.[221] Thus, it seems reasonable to estimate that about 88 million records are breached per year.[222]

---

[217] If this number underestimates the real number, it will not change a result that shows the rate of identity fraud to be too low to justify awarding data monitoring damages (because a more accurate, higher number would reduce that rate even more).

[218] The year 2005 was chosen because that was when most states started to require data breach notification. *Cf.* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1118 nn.21–22 (2008).

[219] *See* discussion *supra* note 208.

[220] *See* OSF Database, *supra* note 216 (sorting and summing total affected records from 2005 through 2008).

[221] OPEN SECURITY FOUNDATION, DATA LOSS DATABASE 2008 YEARLY REPORT, http://datalossdb.org/yearly_reports/dataloss-2008.pdf (last visited Oct. 5, 2009). This number, however, does not include the Heartland Payment Systems breach, which compromised an unknown—but possibly huge—number of records. *See* Dash & Stone, *supra* note 215, at B4.

[222] By comparison, the Identity Theft Resource Center reported 127.7 million records exposed in 2007 as well as incidents in 2006 and 2005 affecting "potentially" 19 million and 64.8 million "individuals," respectively. IDENTITY THEFT RESOURCE CTR., 2007 BREACH LIST 1 (2008), http://www.idtheftcenter.org/ITRC%20Breach%20Report%202007.pdf [hereinafter 2007 ITRC Breach Report]; IDENTITY THEFT RESOURCE CTR., 2006 DISCLOSURES OF U.S.

[63] The other component of the calculation is the number of identity fraud cases caused by data breach. This is a two-part figure based on the total number of identity fraud cases multiplied by the percentage of those cases caused by data breach. About eight to ten million people suffer identity fraud annually.[223] Estimates of the percentage of identity fraud resulting from company-controlled data range from 12% to 26.5%.[224] Data breach directly counts for about 5% to 11%.[225] Thus, the amount of

DATA INCIDENTS 1 (2007), http://idtheftmostwanted.org/ITRC%20Breach%20Report%202006.pdf [hereinafter 2006 ITRC Breach Report]; IDENTITY THEFT RESOURCE CTR., 2005 DISCLOSURES OF U.S. DATA INCIDENTS 1 (2006), http://idtheftmostwanted.org/ITRC%20Breach%20Report%202005.pdf [hereinafter 2005 ITRC Breach Report]. The ITRC numbers do not include some breaches that could potentially expose sensitive data but where "no actionable incident has been documented or disclosed." *Id.*

[223] *See* 2009 Javelin Survey, *supra* note 183, at 5 (noting that "almost 10 million Americans learned they were victims of identity fraud in 2008"); 2006 FTC Survey, *supra* note 179, at 4 (extrapolating survey statistics to show that approximately 8.3 million people suffered identity fraud in 2005).

[224] *See* SASHA ROMANOSKY ET AL., DO DATA BREACH DISCLOSURE LAWS REDUCE IDENTITY THEFT? 8–9 (2008), http://weis2008.econinfosec.org/papers/Romanosky.pdf. These figures include any forms of data loss where a company arguably had control of the data, including theft by corrupt business employees, misuse of data from purchase or other transactions, and direct theft of the information from the company. *Id*. at 9 n.19; *see also* 2009 Javelin Survey, *supra* note 183, at 7; 2006 FTC Survey, *supra* note 179, at 30. The CIMIP study found that in the cases in which the source of data was known, business-controlled data accounted for half of them. *See* 2007 CIMIP Report, *supra* note 183, at 53. That scales to 26.5% of all cases in that survey, when unknown cases are also included. *See id.* at 10, 53 (noting that a point of compromise could be determined in 274 out of 517 cases); ROMANOSKY, *supra* at 8–9.

[225] *See* 2009 Javelin Survey, *supra* note 183, at 7 (reporting that eleven percent of survey respondents who knew where misused data came from believed that the data was from a data breach); 2006 FTC Survey, *supra* note 179, at 30 (where five percent of respondents said that information used in an identity fraud was obtained through a data breach). However, most respondents in both surveys did not know how their data was obtained. *See* 2009 Javelin Survey, *supra* note 183, at 7 (disclosing that its figures were based on the thirty five percent of respondents who they knew how their data was obtained, out of all 482 respondents who reported suffering identity fraud); 2006 FTC Survey, *supra* note

identity fraud resulting from data breach might be in the range of 415,000 to 1 million incidents per year.[226] A calculation of all identity frauds and all forms of data breach yields a 0.5% to 1% rough estimate of the rate at which data breach results in identity fraud.[227]

[64] But not all types of data breach are the same. As shown in Table 1, the forms of data breach can be categorized by whether they resulted from an intentional or unintentional act, and whether they likely exposed data to a third party. Some forms of data breach appear more likely to lead to data misuse and, thus, to identity fraud. In particular, fraud may be more likely when data is intentionally exposed. Misplaced backup tapes, lost laptops and stolen hardware seem less likely to result in data misuse. Some research supports this intuition. For example, a GAO study of twenty-four large breaches was able to find data misuse in only four of those cases, all of which involved hacking or misrepresentation.[228]

179, at 30 (showing results that fifty six percent of survey respondents didn't know how their information was taken).

[226] Using the numbers in the 2006 FTC Survey, five percent of 8.3 million breaches would be 415,000 incidents attributable to data breach. *See* 2006 FTC Survey, *supra* note 179, at 4, 30. The Javelin numbers are eleven percent of "nearly" ten million breaches, or 1.1 million incidents, rounded down to one million to allow for the word "nearly." *See* 2009 Javelin Survey, *supra* note 183, at 5, 7.

[227] *See* discussion *supra* notes 220, 226 and accompanying text (dividing the FTC and Javelin numbers by the estimated number of records breached from 2005 through 2008).

[228] *See* 2007 GAO Report, *supra* note 15, at 24, 26.

	Intentional Act	Unintentional Act
Data Exposed	Fraud, Hacking, Social Engineering, Viruses, Stolen Documents	Accidental disclosure through mail, Internet, or e-mail
Data Not Exposed	Stolen media, backup tapes, or computer	Lost documents, drives, computers, or media Improperly disposed documents, drives, computers, or media

Table 1: Forms of Data Breach

[65] Data breach likelihood calculations should consider this. A plaintiff who seeks monitoring costs following a hacking-related breach probably has a greater chance of suffering identity fraud than a plaintiff who sues after a laptop is lost; their claims should not be treated the same. Likewise, as discussed in Part V.A, not all forms of identity fraud have the same cost. Existing-account fraud, especially on credit-card accounts, presents a particularly low risk for the consumer because of laws limiting liability.[229] Therefore, the appropriate calculation might not be the total amount of identity fraud resulting from all data breaches, but rather, the rate at which new account fraud results from intentional, data-exposing breaches such as hacking, social engineering, and fraud.

[66] The more focused calculation increases the probability estimate. From 2005 through 2008, about 4.8 million Social Security number records per year were compromised in data breaches that involved hacking, social engineering or fraud.[230] About one in five identity fraud

[229] *See* discussion *supra* note 181.

[230] The OSF database, when filtered to report only totals for Fraud and Hacking events, shows forty-six million records in 2005, 8.5 million records in 2006, 121 million records in 2007, and 20.7 million records in 2008, for total of 196.2 million records. *See* OSF Database, *supra* note 216. When those results are further filtered to show only breaches that disclose Social Security numbers, the type of data most useful in new account fraud,

cases are new-account frauds.[231] If 5% to 11% of those are the result of data breach,[232] then somewhere around 100,000 to 170,000 new account fraud cases result from fraud and hacking incidents each year.[233] Dividing the 170,000 by 4.8 million gives about one in twenty-eight estimated chance (or 3.5% probability) that a record in a data breach involving fraud or hacking of Social Security numbers will be used for new account fraud.

C. COST AND EFFECTIVENESS OF REMEDIAL MEASURES

[67] Several methods exist to try to mitigate the effects of data loss. This section discusses some of the more common data loss remediation measures, their costs, and their effectiveness at avoiding loss.

1. CREDIT MONITORING

[68] Credit monitoring is one of the most common reactions to data loss. It has become common practice for organizations to offer free credit monitoring after a breach; the monitoring is usually offered for a limited period, such as a year or two.[234] As discussed in Part II.A, plaintiffs have also sought—without success—to recover the costs of additional credit monitoring beyond the free period.

---

the total number of accounts affected since 2005 drops to 19.2 million. Calculating that as an annualized number gives 4.8 million per year.

[231] *See* 2006 FTC Survey, *supra* note 179, at 4, 12 (showing 0.8% of respondents claiming new account fraud, representing 22% out of the 3.7% who reported some form of identity fraud); 2005 BJS Survey, *supra* note 181, at 1 (showing that 1,083,100, or 16.85%, of the 6,426,200 estimated households that reported any form of identity fraud reported new account fraud).

[232] *See* discussion *supra* note 225. Note that this simple calculation ignores the real possibility that data breaches could be disproportionately responsible for new account fraud.

[233] Using the FTC numbers gives 21.6% of 415,000 = 89,640. *See supra* notes 226, 231. Combining the BJS numbers with Javelin's higher estimate for the number of frauds resulting from data breach gives 16.85% of 1,000,000 = 168,500. *See supra* note 231.

[234] 2007 GAO Report, *supra* note 15, at 35.

[69] Offered primarily by the three credit reporting bureaus, credit monitoring products allow increased access to credit reports. Although the Fair Credit Reporting Act entitles everyone to one free credit report per year,[235] credit monitoring enables unlimited access to one's credit report and, optionally, credit score.[236] The services typically alert the subscriber when credit information changes.[237] Credit monitoring often includes identity theft insurance, which promises to pay for certain costs of responding to identity fraud.[238] Each credit reporting bureau offers credit monitoring products that monitor only its own credit reports, or, for a higher price, products that monitor all three credit bureau reports.[239] Credit monitoring services that monitor all three bureaus currently cost about fifteen dollars per month.[240]

---

[235] 15 U.S.C. § 1681j(a)(1)(A) (2006).

[236] *See* Credit Monitoring, http://www.thecredittruth.org/credit-monitoring.aspx (last visited Oct. 5, 2009).

[237] For example, Equifax lists the following types of notifications customers of its credit monitoring service could expect to receive: "New accounts opened in your name; credit inquiries resulting from a company requesting a copy of your credit report; an address change; bankruptcies and other public records; some changes to current accounts; balance increase alerts based on a self-selected dollar amount or percentage." Equifax Credit Watch FAQs, http://www.equifax.com/cs/Satellite/EFX_Content_C1/1175248697129/5-1/5-1_Layout.htm (last visited Oct. 5, 2009).

[238] *See* Consumer Reports Money Adviser, *Costly Credit-Monitoring Services Offer Limited Fraud Protection*, http://www.consumerreports.org/cro/money/credit-loan/costly-credit-monitoring-services-offer-limited-fraud-protection-4-07/overview/0704_costly-credit-monitoring-services-offer-limited-fraud-protection_ov.htm?Extkey=SY95PI0&CMP=KNC-CROVMYSSP&HBX_OU=51&PK=yssp (last visited Oct. 5, 2009).

[239] *See, e.g.*, Equifax 3-in-1 Monitoring With 4 FICO Scores, http://www.equifax.com/3in1-monitoring-with-4-fico-scores (last visited Oct. 5, 2009); Triple Advantage, http://www.experian.com/consumer-products/triple-advantage.html (last visited Oct. 5, 2009); TrueCredit, http://www.truecredit.com/3BCM?AID=104475848-PID=19119618-SID=-credit-report-monitoring-truecredit_review.php--2009-09-21--23-44-05 (last visited Oct. 5, 2009).

[240] *See, e.g.*, Equifax 3-in-1 Monitoring With 4 FICO Scores, http://www.equifax.com/3in1-monitoring-with-4-fico-scores (last visited Oct. 5, 2009);

[70] Although popular, credit monitoring products have a number of problems. They only notify subscribers when something bad has already happened; this allows quicker response to a fraud, but does not prevent the fraud.[241] Credit monitoring only monitors financial information that appears on a credit report.[242] If data is misused non-financially or in a way that is not tied to the consumer's social security number, credit monitoring will not detect it.[243] Credit monitoring, therefore, is useless against illegal use of a social security number to avoid tax or employment laws, when given to a law enforcement officer during arrest, or in medical identity fraud.[244] Credit monitoring also cannot detect unauthorized charges on existing accounts.[245] Finally, the insurance included in credit monitoring products can be less than valuable due to limitations and gaps in coverage.[246]

[71] For these reasons, credit monitoring has limited usefulness. As such, courts have failed to find such monitoring to be reasonably necessary.

Triple Advantage, http://www.experian.com/consumer-products/triple-advantage.html (last visited Oct. 5, 2009); TrueCredit, http://www.truecredit.com/3BCM?AID=104475848-PID=19119618-SID=-credit-report-monitoring-truecredit_review.php--2009-09-21--23-44-05 (last visited Oct. 5, 2009).

[241] *See* Kelli B. Grant, *4 Reasons to Forego Credit Monitoring Services*, SMARTMONEY, July 14, 2008, http://www.smartmoney.com/spending/deals/4-reasons-to-forgo-credit-monitoring-services-23454.

[242] *See* Collins, *supra* note 182; Privacy Rights Clearinghouse, Straight Talk About Identity Theft Monitoring Services, http://www.privacyrights.org/fs/fs33-CreditMonitoring.htm (last visited Oct. 5, 2009).

[243] *See* Collins, *supra* note 182; Privacy Rights Clearinghouse, *supra* note 242.

[244] Privacy Rights Clearinghouse, *supra* note 242.

[245] *Id.*

[246] *See* Consumer Reports Money Adviser, *supra* note 238.

2. CREDIT FREEZES

[72] The credit freeze is another option for people worried about identity fraud. A credit freeze blocks all access to a consumer's credit report, preventing, rather than merely monitoring, new account fraud as long as the freeze is active.[247] A credit freeze prevents fraudulent new accounts in the consumer's name because the seller of services cannot check the consumer's credit report.[248] Freezing credit reports first became an option with the passage of several state laws; the credit reporting bureaus responded with plans to announce nationwide credit freeze availability.[249]

[73] Although laws in forty-seven states and the District of Columbia allow consumers to freeze their credit reports,[250] the laws differ on how

---

[247] *See* Security Freeze, http://www.experian.com/consumer/security_freeze.html (last visited Oct. 5, 2009).

[248] *See* Eve Mitchell, *Putting Freeze on Identity Theft*, CONTRA COSTA TIMES (Cal.), Nov. 12, 2007.

[249] Jane J. Kim, *More People Are Freezing Credit Reports; Fearful of ID Theft; Consumers Block Access to Their Records; A Quick Thaw, Made Easier*, WALL ST. J., Oct. 24, 2007, at D1.

[250] *See* ALASKA STAT. §§ 45.48.010–.995 (Westlaw 2009); ARIZ. REV. STAT. ANN. § 44-1698 (Supp. 2008); ARK. CODE. ANN. §§ 4-112-101 to 4-112-113 (Supp. 2007); CAL. CIV. CODE § 1785.11.2 (West Supp. 2008); COLO. REV. STAT. ANN. § 12-14.3-106.6 (West Supp. 2008); CONN. GEN. STAT. ANN. §§ 36a-701 to 36a-701a (Supp. 2008); DEL. CODE ANN. tit. 6, §§ 2201–2203 (Supp. 2006); 2007-3 D.C. Code Adv. Leg. Serv. 33–39 (LexisNexis); FLA. STAT. ANN. § 501.005 (West Supp. 2008); GA. CODE ANN. §§ 10-1-913 to -915 (Supp. 2008); HAW. REV. STAT. § 489P-3 (LexisNexis Supp. 2007); IDAHO CODE ANN. §§ 28-52-101 to -109 (Supp. 2008); 815 ILL. COMP. STAT. ANN. 505/2MM (West 2008); IND. CODE ANN. §§ 24-5-24-1 to -18 (West Supp. 2008); IOWA CODE ANN. §§ 714G.1–.11 (West, Westlaw through 2008 Reg. Sess.); KAN. STAT. ANN. §§ 50-702(j), 50-723, 50-724 (Supp. 2007); KY. REV. STAT. ANN. § 367.365 (LexisNexis 2008); LA. REV. STAT. ANN. §§ 9:3571.1(H)(5), 9:3571(M)–(Y) (Supp. 2008); ME. REV. STAT. ANN. tit., 10 §§ 1312(10-C), 1313-C to –E (Supp. 2007); MD. CODE ANN., COM. LAW § 14-1212.1 (LexisNexis Supp. 2005); MASS. GEN. LAWS ANN. ch. 93 §§ 50, 56(b), 62A (West Supp. 2008); MINN. STAT. §§ 13C.016–.019 (2008); MISS. CODE ANN. §§ 75-24-201 to -217 (Supp. 2007); MONT. CODE ANN. § 30-14-1726 to -1736 (2007); NEB. REV.

much the consumer must pay to freeze or unfreeze the report.[251] Most laws allow identity fraud victims to freeze or unfreeze their credit reports for free.[252] Depending on the jurisdiction, consumers who are not victims of identity fraud may have to pay to place a freeze,[253] remove a freeze,[254]

STAT. ANN. §§ 8-2601 to -2615 (Supp. 2008); NEV. REV. STAT. ANN. §§ 598C.105, 598C.300–.390 (LexisNexis Supp. 2007); N.H. REV. STAT. ANN. §§ 359-B:22 to :26 (LexisNexis Supp. 2007); N.J. STAT. ANN. §§ 56-11-46 to -50 (West Supp. 2008); N.M. STAT. ANN. §§ 56-3A-01 to -06 (West Supp. 2008); N.Y. GEN. BUS. LAW § 380-t (McKinney Supp. 2008); N.C. GEN. STAT. ANN. § 75-63 (2007); N.D. CENT. CODE §§ 51-33-01 to -14 (2007); OHIO REV. CODE ANN. § 1349.52 (West, Westlaw through 2008 File 129); OKLA. STAT. tit. 24, §§ 149–159 (West 2008); ORE. REV. STAT. ANN. §§ 646A.606–.618, 646A.624 (West Supp. 2008); 73 PA. STAT. ANN. §§ 2501–2510 (West 2008); R.I. GEN. LAWS §§ 6-48-1 to -7 (Supp. 2008); Financial Identity Fraud and Identity Theft Protection Act, 2008 S.C. Act 190 (to be codified at S.C. CODE ANN. §§ 37-20-110(16), 37-20-160); S.D. CODIFIED LAWS §§ 54-15-1 to -16 (Supp. 2008); TENN. CODE ANN. §§ 47-18-2101 to -2110 (Supp. 2008); TEX. BUS. & COM. CODE ANN. §§ 20.034–.04 (Vernon Supp. 2008); UTAH CODE ANN. §§ 13-45-101 to -401 (Supp. 2008); VT. STAT. ANN. tit. 9, § 2480h (2006); VA. CODE ANN. §§ 59.1-444.1 to -444.2 (Supp. 2008); WASH. REV. CODE ANN. § 19.182.170 (West 2007); W. VA. CODE ANN. §§ 46A-6L-101 to -105 (LexisNexis Supp. 2008); WIS. STAT. ANN. § 100.54 (West Supp. 2008); WYO. STAT. ANN. §§ 40-12-501 to -509 (2007).

[251] Letter from Jeannine Kenney & Gail Hillebrand, Senior Policy Analyst & Senior Attorney, Consumers Union, to Federal Trade Commission (Feb. 25, 2008), at 5, *available at* http://www.consumersunion.org/pdf/FTC-Comments-Security-Freeze.pdf.

[252] *See* CHRISTOPHER WOLF, PROSKAUER ON PRIVACY § 5:5.5[B][11] (2009) (Tanya L. Forsheit & Kristen J. Mathews eds. 2009) (2006).

[253] *See, e.g.*, DEL. CODE ANN. tit. 6 § 2203(b)(13) (2009) (allowing a twenty dollar charge for a consumer's initial credit freeze, after which all freeze-related activity must be free); NEB. REV. STAT. ANN. §§ 8-2607 to -2609 (Supp. 2008) (allowing a $3 fee to place a freeze, with free removal or temporary lifting of the freeze); VA. CODE ANN. § 59.1-444.2 (Supp. 2008) (allowing a ten dollar fee to place a freeze, but no fee for removal or temporary lifting).

[254] *See, e.g.*, COLO. REV. STAT. ANN. § 12-14.3-106.6(12)(c) (West Supp. 2008) (allowing a ten dollar fee to remove a freeze, but no fee to place the freeze); N.Y. GEN. BUS. LAW § 380-t (n)(2) (McKinney Supp. 2008) (allowing a five dollar fee to remove or temporarily lift a freeze, but no fee to place the first freeze).

both,[255] or neither.[256] Consumers in some states may also temporarily freeze their credit reports for less than the cost of placing and then lifting a freeze.[257]

[74] Credit freezes are no panacea, but they are more effective than credit monitoring.[258] As with credit monitoring, credit freezes cannot prevent existing account fraud or forms of identity fraud that do not require credit.[259] Credit freezes can also be more of a hassle than credit monitoring. Unlike the all-in-one credit monitoring services, a credit freeze must be placed separately with each reporting bureau.[260] Placing or lifting a freeze takes time, so consumers with frozen credit cannot get "instant credit" or other loans unless they plan ahead by lifting the

[255] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1698(K) (Supp. 2008) (allowing a five dollar fee to place, remove, or temporarily lift a freeze); CAL. CIV. CODE § 1785.11.2(m) (West Supp. 2008) (allowing credit bureaus to charge a ten dollar fee to place or remove a freeze); GA. CODE ANN. § 10-1-914(p) (Supp. 2008) (allowing a three dollar fee to place, remove, or temporarily lift a freeze); TENN. CODE ANN. § 47-18-2108(*l*) (Supp. 2008) (allowing a $7.50 fee to place a freeze, a five dollar fee to remove the freeze, and no fee to temporarily lift a freeze).

[256] *See, e.g.*, IND. CODE ANN. § 24-5-24-14 (West Supp. 2008); Financial Identity Fraud and Identity Theft Protection Act, 2008 S.C. Act 190, sec. 2, § 37-120-160(J), *available at* http://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm.

[257] *See, e.g.*, CAL. CIV. CODE § 1785.11.2(m) (West Supp. 2008); CONN. GEN. STAT. ANN. § 36a-701a(i) (Supp. 2008) (allowing a ten dollar fee to temporarily lift a credit freeze).

[258] *See, e.g.*, Manny Vetti, *Credit Freeze Or Credit Monitoring? Best Ways to Fight Identity Theft*, http://ezinearticles.com/?Credit-Freeze-Or-Credit-Monitoring?--Best-Ways-to-Fight-Identity-Theft&id=1389620 (last visited Oct. 5, 2009).

[259] *Cf.* Mitchell, *supra* note 248 (noting that "access to a consumer's *credit* reports and *credit* scores cannot be shared" unless specific permission is given) (emphasis added).

[260] Claire Moore, *Security Freeze or Fraud Alert*, Aug. 30, 2009, http://www.examiner.com/x-6044-Financial-Literacy-Examiner~y2009m8d30-Security-freeze-or-fraud-alert (last visited Oct. 5, 2009).

freeze.[261] The reporting bureaus also make the credit freeze process relatively difficult, often forcing the consumer to "jump through hoops" to freeze their credit files.[262]

[75] Security freezes are also cheaper than credit monitoring. Even in states where placing and lifting a credit freeze is the most expensive, a consumer can place and temporarily lift a credit freeze several times for the cost of three-bureau credit monitoring.[263] Perhaps the low cost of placing credit freezes explains why plaintiffs do not seek damages resulting from the cost of placing credit freezes.[264]

3. FRAUD ALERTS

[76] Fraud alerts are another possible response to data loss. The Fair and Accurate Credit Transactions Act (FACTA) of 2003 included provisions enabling fraud alerts.[265] A fraud alert is a statement in a credit

[261] Business advocacy groups have been quick to cite this barrier to instant credit as one of the problems with credit freeze laws. *See, e.g.*, Minn. Senate, Commerce Committee Update, Apr. 3, 2006, http://www.senate.leg.state.mn.us/committee/2005-2006/commerce/update.htm (reporting Minnesota Business Association comments that a proposed credit freeze law could cause problems with instant credit).

[262] *See* Marni Ginther, *Icy Start for Credit Freeze*, ST. PAUL PIONEER PRESS, Oct. 23, 2006, at 1A.

[263] The states in which credit freezes are most expensive allow credit bureaus to charge ten dollars per bureau for placing or removing a freeze, and twelve dollars to temporarily lift a freeze. *See* IOWA CODE ANN. § 714G.5 (West 2008). For the $180 annual price of three-bureau credit monitoring, a consumer in these states could place a freeze then temporarily lift it four times per year. Most states are cheaper. For example, residents of Minnesota, which caps credit freeze fees at five dollars, could place a credit freeze and temporarily lift it at all three bureaus ten times per year for the same price as a credit-monitoring service. *See* MINN. STAT. § 13C.016, subdiv. 8 (2008). *See also supra* note 240 and accompanying text.

[264] Security freezes may also be underutilized by fraud victims. According to the 2006 FTC identity theft survey, only seven percent of victims of identity fraud froze their credit reports. 2006 FTC Survey, *supra* note 179, at 48.

[265] 15 U.S.C. § 1681c-1(a)(1) (2006).

file that tells anyone looking at it that "the consumer may be a victim of fraud."[266] An initial fraud alert, which can be activated by anyone who "asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime,"[267] lasts for ninety days.[268] An extended fraud alert lasts for seven years,[269] but is only available to consumers who have suffered identity fraud.[270] Prospective creditors who receive a credit report tagged with an initial fraud alert must use "reasonable policies and procedures" to "form a reasonable belief" that the request is authorized.[271] If the credit report is tagged with an extended alert, then the prospective creditor must contact the consumer in person or by phone to confirm her application.[272]

[77] The greatest weakness in this system, from the victim's perspective, is that a fraud alert is only available for ninety days, unless the victim has already suffered fraud.[273] A few enterprising souls have attempted to fix this problem with businesses that repeatedly place initial fraud alerts on a consumer's credit record, essentially creating a continuous fraud alert for as long as the consumer pays for the service.[274]

---

[266] *Id.* § 1681a(q)(2).

[267] *Id.* § 1681c-1(a)(1).

[268] *Id.* § 1681c-1(a)(1)(A). The consumer may request that the fraud alert be removed before the ninety-day period. *Id.*

[269] *Id.* § 1681c-1(b)(1)(A). The consumer can also request an early end to an extended fraud alert.

[270] *Id.* § 1681c-1(b)(1).

[271] *Id.* § 1681c-2(h)(1)(B). An open-end credit plan may be extended without this check. *Id*.

[272] *Id.* § 1681c-2(h)(2)(B). Open-end credit plans are not subject to this requirement, either. *Id.*

[273] *See* discussion *supra* note 230 and accompanying text.

[274] *See* Ron Lieber, *Outspoken Champion of Identity Protection Tussles With Skeptics*, N.Y. TIMES, May 24, 2008, at C1 (discussing LifeLock).

The most notorious of these services, LifeLock, has drawn legal trouble from its customers,[275] the state of Oklahoma,[276] and Experian.[277]

[78] Fraud alerts also share a problem with credit monitoring and credit freezes. Fraud alerts do no protect against non-financial forms of fraud and cannot prevent unauthorized charges to existing accounts.[278] But unlike credit monitoring and credit freezes, fraud alerts are free.[279] Despite that advantage, few identity fraud victims have used fraud alerts.[280]

D. PUTTING THE NUMBERS TOGETHER

[79] The available data shows that:

- The average overall cost of new account fraud is anywhere from $1620 to $49,941 per victim.[281]

[275] Associated Press, *Lifelock Customers Sue Owners, Cry Fraud*, May 23, 2008, *available at* http://www2.journalnow.com/content/2008/may/23/lifelock-customers-sue-owner-cry-fraud/business-nationworld.

[276] Lieber, *supra* note 274. Oklahoma claims that LifeLock is selling insurance without a license through its one million dollar guarantee. *Id.*

[277] *Id.*

[278] *See* FED. TRADE COMM'N, TO BUY OR NOT TO BUY: IDENTITY THEFT SPAWNS NEW PRODUCTS AND SERVICES TO HELP MINIMIZE RISK 1–2 (2007), http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.pdf.

[279] *See* § 1681c-1(a)(1), 1681c-1(b)(1) (requiring initial and extended fraud alerts to be placed "upon . . . request").

[280] *See* 2006 FTC Survey, *supra* note 179, at 46–48 (showing that only fourteen percent of victims placed an initial ninety-day fraud alert with a credit agency, and only seven percent placed seven-year extended alerts).

[281] *See* discussion *supra* Part V.A.

- The largest estimated probability that an intentional data breach involving a Social Security Number will lead to new-account identity fraud is roughly one in twenty-eight, or 3.5%.[282]

- Available means of reducing new account identity fraud have mixed effectiveness.[283]

[80] Most plaintiffs have sought credit monitoring as their form of relief.[284] The cheapest three-bureau credit monitoring service costs $180 per year.[285] To buy just five years of credit monitoring beyond the one or two years most organizations offer for free after a breach, a data breach victim would have to pay $900.[286] Suppose, for the sake of argument, that (1) credit monitoring is one hundred percent effective at preventing new account fraud; (2) that the ITRC is right about the cost of new account identity fraud being nearly $50,000; and (3) that the one in twenty-eight chance of a hack leading to new-account identity fraud is in the ballpark of accurate.[287]

---

[282] *See* discussion *supra* Part V.B.

[283] *See* discussion *supra* Part V.C.

[284] *See* discussion *supra* Part II.A.

[285] *See* Triple Advantage, *supra* note 239.

[286] The five-year example period was chosen as a potentially reasonable time period for credit monitoring. Data monitoring plaintiffs' complaints have not specified how long they thought credit monitoring should last. *See, e.g.*, First Amended Class Action Complaint and Jury Demand at 13, Kahle v. Litton Loan Servicing, L.P., 486 F. Supp. 2d 705 (S.D. Ohio 2007) (No. 1:05CV756), 2006 WL 430509 (seeking an order requiring the defendant to "establish a credit monitoring program"); Complaint at 11, Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006) (No. 1:05-cv-00767), 2005 WL 3518203 (seeking "[d]amages sufficient to pay for the monitoring of credit reports and accounts"); Complaint and Jury Demand at 15, Giordano v. Wachovia Secs., L.L.C., No. 06-476, 2006 WL 2177036 (D. N.J. July 31, 2006) (No. AT2-L-3567-05), 2005 WL 4255487 (seeking an order requiring the defendant to "establish a credit monitoring program").

[287] This clearly is not the case, but it is the simplest way to proceed, and makes little difference in the final result.

[81] Based on these suppositions, the expected cost of a breach would be $1770 per person. Five years of credit monitoring costs a little over half as much as the expected cost of the breach.[288] To economically justify allowing data monitoring costs, the aggregate cost savings should be significant enough to overcome any doubt that the cost savings are real and outweigh other drawbacks. This hypothetical illustrates that there is no such savings with post-breach credit monitoring.

[82] The hypothetical uses numbers that were as favorable to maximizing the expected value of loss as reasonably possible. For example, the total amount of breached data was probably an underestimate.[289] The total cost of new-account identity fraud, $50,000, was an order of magnitude higher than other estimates of these costs.[290] The credit monitoring cost was calculated using the least expensive service available. The calculation also assumed that credit monitoring completely prevents identity fraud. Yet, even with these favorable numbers, the cost factors still do not support recovery for credit monitoring costs after a data breach.[291] Given available data, it isimpossible to construct a calculation favoring recovery that does not strain credulity.[292]

---

[288] *See* discussion *supra* Part V.C.1.

[289] *See* discussion *supra* notes 213–16 and accompanying text.

[290] *See* discussion *supra* notes 198–201 and accompanying text.

[291] Note again that these costs are based on averages and aggregates. Some individual data breach victims will suffer identity fraud that will cost them tens of thousands of dollars. The FTC's data suggests that at least ten percent of identity fraud victims will lose more than ten thousand dollars. *See* 2006 FTC Survey, *supra* note 179, at 5. But these individual cases do not make for an overall aggregate economic benefit in allowing medical monitoring costs.

[292] The most favorable calculation possible would assume that: (1) the average cost of new-account identity fraud is $50,000; (2) credit monitoring is 100% effective at eliminating the risk of identity fraud; and (3) all or most of the unknown causes of identity fraud in the FTC and Javelin surveys are data breaches, and fifty-six percent of annual identity frauds are the result of data breaches. *See* 2006 FTC Survey, *supra* note 179, at 30. In that case, the probability that a data breach involving fraud or hacking of

VI. CONCLUSION

[83] The courts that have rejected post-breach credit monitoring claims are right, but for the wrong reasons. Recovery for monitoring after data breach should be denied, not because data breach is insufficiently like exposure to toxins, but because plaintiffs have not shown that these measures are reasonably necessary. The relationship between the cost of monitoring, the potential cost of identity fraud, and the likelihood that data breach will lead to identity fraud suggests that it is currently only slightly more expensive, at worst, to wait for identity fraud than to pay for monitoring up-front. But this could change over time, especially for intentional forms of data compromise. Instead of dismissing these claims for insufficient similarity to medical claims, courts should evaluate them based on whether the remedial measures are reasonably necessary, weighing such factors as cost effectiveness of those measures and placing the burden on the plaintiff to show reasonable necessity.

Social Security numbers will lead to new-account fraud would be 23.3% (5.6 million identity frauds x .20 ratio of new-account frauds to total identity frauds)/4.8 million fraud or hacking data breaches that involve Social Security numbers). With all those stars aligned, the expected cost of a data breach would be $11,666, but the assumptions needed to get to that number stretch too far. If the cost of new-account identity fraud is closer to the $4850 the BJS survey found, the expected cost of a breach drops to $1130—only $230 more than the cost of five years of the lowest-price credit monitoring. *See* 2005 BJS Survey, *supra* note 181, at 5.